

# Projekt PSeAP

## Opis Przedmiotu Zamówienia – GW (OPZ-GW)

Dokument:

**PSeAP\_OPZ-GW\_121015D**

Ostatni człon nazwy pliku wskazuje na datę powstania dokumentu w formacie RRMMDDx i jest zarazem numerem jego wersji.

Ten dokument nie podlega kontroli zmian. Zostanie on użyty jednorazowo, wyłącznie na potrzeby określenia szacowanej wartości zamówienia.

Ten dokument nie podlega formalnemu zatwierdzeniu.

wersja	Autor	data przyjęcia	Koordynator Projektu
121015D	InfoStrategia K. Heller i A. Szczerba sp. jawna		Konrad Łoboda

---

## **SPIS TREŚCI**

<b>1</b>	<b>WPROWADZENIE .....</b>	<b>7</b>
1.1	Cel dokumentu .....	7
1.2	Opis Projektu .....	7
<b>2</b>	<b>SŁOWNIK DEFINICJI I SKRÓTÓW .....</b>	<b>9</b>
2.1	Definicje pojęć .....	9
2.2	Definicje skrótów .....	12
<b>3</b>	<b>PRZEDMIOT ZAMÓWIENIA .....</b>	<b>13</b>
<b>4</b>	<b>HARMONOGRAM REALIZACJI .....</b>	<b>14</b>
<b>5</b>	<b>WYMAGANIA OGÓLNE DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA .....</b>	<b>17</b>
5.1	Wymagania dotyczące bezpieczeństwa .....	17
5.2	Wymagania dotyczące wydajności i pojemności .....	17
5.3	Wymagania ogólne dotyczące wdrożenia .....	18
5.3.1	Analiza przedwdrożeniowa .....	18
5.3.2	Dostawa, instalacja i konfiguracja sprzętu i oprogramowania .....	20
5.3.3	Pilotaż .....	20
5.3.4	Środowisko testowe i testy funkcjonalne Systemu .....	22
5.3.5	Konfiguracja i produkcyjne uruchomienie systemu PSeAP .....	23
5.3.6	Instruktaż stanowiskowy .....	24
5.4	Wymagania prawne .....	28
5.5	Równoważność rozwiązań .....	31
5.6	Wymagania w zakresie dokumentacji .....	32
5.7	Inne wymagania ogólne .....	34

---

<b>6</b>	<b>ARCHITEKTURA I GŁÓWNE KOMPONENTY .....</b>	<b>35</b>
<b>7</b>	<b>USŁUGI PUBLICZNE SYSTEMU .....</b>	<b>38</b>
7.1	Usługi przewidziane do wdrożenia w ramach projektu PSeAP .....	38
7.2	Wdrożenie e-usług.....	64
<b>8</b>	<b>SYSTEM E-USŁUG INTERNETOWYCH .....</b>	<b>65</b>
8.1	System zarządzania i monitoringu infrastruktury .....	65
8.1.1	System zarządzania incydentami .....	65
8.1.2	System wirtualizacji środowiska serwerów .....	66
8.1.3	System wirtualizacji środowiska serwerów- wymagania dodatkowe .....	68
8.1.4	System tworzenia kopii zapasowych (backupu) .....	68
8.1.5	System optymalizacji dostępu .....	70
8.1.6	System operacyjny.....	71
8.1.7	Baza danych .....	71
8.2	Portal e-Usług .....	71
8.3	Centralny Portal Internetowy .....	76
8.4	Wdrożenie e-usług.....	85
8.5	Wdrożenie SeUI .....	87
<b>9</b>	<b>SYSTEM ELEKTRONICZNEGO OBIEGU DOKUMENTÓW .....</b>	<b>90</b>
9.1	Opis podstawowych wymagań i zakres funkcjonalności .....	90
9.2	Wymagania pozafunkcyjne w zakresie SEOD .....	110
9.3	Wdrożenie SEOD.....	114
9.3.1	Wdrożenie produkcyjne systemu .....	115
9.3.2	Formalne przekazanie SEOD do eksploatacji.....	117
<b>10</b>	<b>OPROGRAMOWANIE STANDARDOWE.....</b>	<b>118</b>

---

<b>10.1</b>	<b>Pakiet biurowy typ I.....</b>	<b>119</b>
<b>10.2</b>	<b>Pakiet biurowy typ II.....</b>	<b>123</b>
<b>10.3</b>	<b>System operacyjny dla komputerów PC.....</b>	<b>125</b>
<b>10.4</b>	<b>Serwerowy system operacyjny z elementami zarządzania .....</b>	<b>128</b>
10.4.1	Zarządzanie środowiskami serwerowymi .....	131
<b>10.5</b>	<b>System zarządzania infrastrukturą i oprogramowaniem .....</b>	<b>131</b>
10.5.1	System zarządzania komponentami.....	133
10.5.2	System automatyzacji zarządzania środowisk IT.....	140
10.5.3	System zarządzania incydentami i problemami .....	140
10.5.4	Ochrona antymalware.....	141
<b>10.6</b>	<b>Licencje dostępne do serwerowego systemu operacyjnego (na użytkownika) .....</b>	<b>143</b>
<b>10.7</b>	<b>Kliencki pakiet antywirusowy .....</b>	<b>143</b>
<b>10.8</b>	<b>Serwer portalu Internetowego .....</b>	<b>145</b>
<b>10.9</b>	<b>Serwer relacyjnej bazy danych.....</b>	<b>150</b>
<b>11</b>	<b>INFRASTRUKTURA SIECIOWA ORAZ SPRZĘTOWA SEUI W URZĘDZIE MARSZAŁKOWSKIM.....</b>	<b>164</b>
<b>11.1</b>	<b>Dostawa sprzętu i urządzeń .....</b>	<b>164</b>
11.1.1	Oznaczenia i definicje.....	164
<b>11.2</b>	<b>Wymagania sprzętowe –szczegółowe .....</b>	<b>168</b>
11.2.1	Obudowa Blade .....	168
11.2.2	Serwer Blade .....	171
11.2.3	Zasób dyskowy systemowy (ZD-S).....	172
11.2.4	Zasób Dyskowy Aplikacji (ZD-A) .....	173
11.2.5	Wymagania dodatkowe .....	176
11.2.6	Urządzenia sieciowe .....	178
11.2.7	System zarządzania infrastrukturą .....	180
11.2.8	Bezpieczeństwo sieci WAN- Zestaw urządzeń bezpieczeństwa sieci dla Centrali. ....	183

11.2.9	Urządzenia do optymalizacji sieci WAN .....	190
11.2.10	System zarządzania incydentami .....	194
<b>12</b>	<b>UZUPEŁNIENIE STRUKTURY SIECIOWEJ URZĘDÓW JST .....</b>	<b>197</b>
<b>12.1</b>	<b>Zakres rzeczowy.....</b>	<b>197</b>
12.1.1	Urządzenia aktywne sieci LAN.....	200
12.1.2	Przełączniki i urządzenia bezpieczeństwa .....	201
12.1.3	Zestawy bezpieczeństwa .....	205
12.1.4	Zestawy bezpieczeństwa typu B.....	213
12.1.5	Urządzenia bezpieczeństwa typu C .....	221
12.1.6	Urządzenia bezpieczeństwa typu D.....	229
12.1.7	Funkcjonalność oprogramowania w urządzeniach bezpieczeństwa typu A,B,C,D .....	237
<b>12.2</b>	<b>Wymagania ogólne dla dostarczanych rozwiązań .....</b>	<b>239</b>
<b>13</b>	<b>WYPOSAŻENIE URZĘDÓW JST W SPRZĘT I URZĄDZENIA .....</b>	<b>241</b>
<b>13.1</b>	<b>Dostawa i uruchomienie serwerów .....</b>	<b>241</b>
<b>13.2</b>	<b>Oznaczenia i definicje .....</b>	<b>241</b>
<b>13.3</b>	<b>Opis wymagań sprzętowych .....</b>	<b>244</b>
13.3.1	Zestaw serwerowy – wariant A .....	244
13.3.2	Zestaw serwerowy – wariant B .....	248
13.3.3	Zestaw serwerowy – wariant C .....	252
<b>13.4</b>	<b>Dostawa i uruchomienie systemu zasilaczy bezprzerwowych (UPS) .....</b>	<b>257</b>
<b>13.5</b>	<b>Dostawa i uruchomienie komputerów osobistych .....</b>	<b>257</b>
13.5.1	Komputery biurowe.....	258
13.5.2	Monitor ciekłokrystaliczny .....	266
13.5.3	Komputery przenośne – „notebook” .....	267
<b>13.6</b>	<b>Zestawy do podpisu elektronicznego .....</b>	<b>273</b>
<b>13.7</b>	<b>Dostawa i uruchomienie infomatów.....</b>	<b>275</b>

---

13.7.1	Obudowa infomatu wewnętrznego .....	275
13.7.2	Jednostka komputerowa infomatu wewnętrznego .....	276
13.7.3	Monitor dotykowy infomatu wewnętrznego .....	280
13.7.4	Obudowa infomatu zewnętrznego.....	282
13.7.5	Jednostka komputerowa infomatu zewnętrznego.....	283
13.7.6	Monitor dotykowy infomatu zewnętrznego .....	283
13.7.7	Oprogramowanie infomatu.....	284
13.7.8	Wdrożenie infomatów .....	295
<b>13.8</b>	<b>Dostawa i uruchomienie urządzeń wielofunkcyjnych .....</b>	<b>296</b>
13.8.1	Zestaw urządzeń wielofunkcyjnych – wymagania wspólne .....	296
13.8.2	Zestaw urządzeń wielofunkcyjnych – wariant A .....	297
13.8.3	Zestaw urządzeń wielofunkcyjnych – wariant B.....	298
13.8.4	Wdrożenie urządzeń wielofunkcyjnych.....	300
<b>13.9</b>	<b>Szafy teleinformatyczne .....</b>	<b>300</b>
<b>14</b>	<b>PROMOCJA PROJEKTU.....</b>	<b>303</b>
14.1	Tablice informacyjne i pamiątkowe .....	303
14.2	Plakietki informacyjne .....	304
14.3	Wymaganie ogólne .....	306
<b>15</b>	<b>GWARANCJE.....</b>	<b>307</b>
<b>16</b>	<b>LICENCJE.....</b>	<b>316</b>
<b>17</b>	<b>INNE DOKUMENTY DO OPRACOWANIA PRZEZ WYKONAWCĘ.....</b>	<b>320</b>
<b>18</b>	<b>SZKOLENIA .....</b>	<b>321</b>

---

---

# 1 Wprowadzenie

## 1.1 Cel dokumentu

Opracowanie niniejsze stanowi Załącznik Nr 7 do SIWZ – opis przedmiotu zamówienia w postępowaniu na wykonanie systemu informatycznego o nazwie: *PSeAP – Podkarpacki System e-Administracji Publicznej*. Zamówienie jest realizowane w ramach projektu *Podkarpacki System e-Administracji Publicznej*, dofinansowanego ze środków Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego.

## 1.2 Opis Projektu

Zgodnie z wnioskiem o dofinansowanie, przedmiotem projektu „PSeAP – Podkarpacki System e-Administracji Publicznej” jest budowa regionalnego środowiska e-Administracji oraz modernizacja infrastruktury teleinformatycznej urzędów administracji samorządowej w województwie podkarpackim. Projekt realizowany jest w partnerstwie przez 160 podmiotów: Województwo Podkarpackie – Lider, Jednostki Samorządu Terytorialnego szczebla powiatowego (14) oraz szczebla gminnego (145).

Projekt zakłada zbudowanie bezpiecznego i skutecznego narzędzia komunikacji pomiędzy interesantem i urzędem w postaci Systemu e-Usług Internetowych (SeUI) zintegrowanego z Systemem Elektronicznego Obiegu Dokumentów (SEOD). Projekt będzie stanowił uzupełnienie i rozszerzenie na poziomie regionu zadań, które będą realizowane centralnie w ramach projektu ePUAP. Oznacza to integrację z platformą ePUAP oraz maksymalne wykorzystanie jej możliwości do udostępniania e-usług przez partnerów projektu.

Rozwiązanie będzie miało dwupoziomową strukturę – SeUI będzie zainstalowany w serwerowni Urzędu Marszałkowskiego Województwa Podkarpackiego w Rzeszowie, natomiast SEOD będzie zainstalowany na serwerach zlokalizowanych w lokalnych jednostkach samorządu terytorialnego biorących udział w projekcie. SEOD będzie instalowany u 157 partnerów, natomiast SeUI będzie obejmowało wszystkich Partnerów Projektu. Oba elementy projektowanego rozwiązania tj. część lokalna i część centralna (regionalna) będą połączone za pośrednictwem bezpiecznego łącza internetowego, opartego o VPN.

Rolą SEOD będzie:

- I) zapewnienie w pełni elektronicznego przetwarzania dokumentów oraz przepływu pracy w jednostkach samorządu terytorialnego uczestniczących w projekcie – system będzie miał możliwość pełnienia roli systemu EKD w rozumieniu rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (*Dz.U. Nr 14, poz. 67*);

- 
- II) wspieranie procesów pracy realizowanych w jednostkach samorządu terytorialnego (automatyzacja przepływu pracy poprzez ścieżki obiegu skonfigurowane w ramach SEOD, a także możliwość integracji z systemami dziedzinowymi z wykorzystaniem interfejsów wymiany danych dostępnych w ramach SEOD);

Rolą SeUI będzie:

- I) świadczenie usług publicznych online na poziomie 1 i 2, informowanie o stanie spraw, punkt dostępowy do usług publicznych na poziomie 3 i 4;
- II) wsparcie i koordynacja procesów wdrażania i aktualizacji e-usług w systemie PSeAP, na platformie ePUAP oraz w ewentualnych zintegrowanych systemach zewnętrznych (Biuletyny Informacji Publicznej, zewnętrzne SEOD);
- III) wsparcie wybranych procesów związanych z utrzymaniem i rozwojem systemu PSeAP realizowanych przez partnerów;

W celu osiągnięcia założonych celów, zaplanowano przeprowadzenie następujących głównych działań:

- I) Zaprojektowanie, wykonanie i wdrożenie Systemu e-Usług Internetowych (SeUI).
- II) Zaprojektowanie, wykonanie i wdrożenie Systemu Elektronicznego Obiegu Dokumentów (SEOD).
- III) Uzupełnienie infrastruktury sieciowej urzędów.
- IV) Budowa infrastruktury sprzętowej SeUI zlokalizowanej w Urzędzie Marszałkowskim.
- V) Wyposażenie urzędów w odpowiedni sprzęt i urządzenia.

Postępowanie na wykonanie systemu informatycznego o nazwie: *PSeAP — Podkarpacki System e-Administracji Publicznej* dotyczy działań 1, 2, 4 i 5 wymienionych powyżej oraz działania 3 (uzupełnienia infrastruktury sieciowej urzędów) wyłącznie w zakresie dostawy instalacji urządzeń aktywnych. Rozbudowa sieci teleinformatycznej oraz dostawa szaf (za wyjątkiem 7 szaf objętych niniejszym postępowaniem) są realizowane w odrębnym postępowaniu.



## 2 Słownik definicji i skrótów

### 2.1 Definicje pojęć

SEOD	<p>System Elektronicznego Obiegu Dokumentów wdrażany u Partnerów w ramach Projektu PSeAP, złożony z dwóch głównych komponentów:</p> <ul style="list-style-type: none"> <li>• EOD – Elektroniczny Obieg Dokumentów</li> <li>• Aplikacja Integrująca, umożliwiającą komunikację EOD z systemami zewnętrznymi</li> </ul> <p>W skład SEOD wchodzi także Oprogramowanie Pomocnicze SEOD.</p>
Centrum Przetwarzania Danych PSeAP, CPD PSeAP	Lokalizacja u Lidera Projektu, gdzie będzie znajdowała się Infrastruktura Sprzętowa SeUI oraz zainstalowane na niej oprogramowanie SeUI (przy czym dopuszcza się możliwość instalacji komponentów lokalnych, wspomagających pracę użytkowników lub systemów Partnera z SeUI, na Infrastrukturze SEOD u Partnerów).
Oprogramowanie Pomocnicze SEOD	Wszelkie oprogramowanie, poza Oprogramowaniem Podstawowym, niezbędne do prawidłowego funkcjonowania SEOD. W szczególności: motor bazy danych, serwer aplikacyjny.
Oprogramowanie Pomocnicze SeUI	Wszelkie oprogramowanie, poza Oprogramowaniem Podstawowym, niezbędne do prawidłowego funkcjonowania SeUI (w szczególności: motor bazy danych).
Oprogramowanie Podstawowe	Systemy operacyjne i sterowniki niezbędne do prawidłowego funkcjonowania Systemu PSeAP, zainstalowane na dostarczonym przez Wykonawcę sprzęcie oraz wszelkie inne oprogramowanie wyspecyfikowane w ramach specyfikacji sprzętu w niniejszym OPZ.
Oprogramowanie autorskie	Oprogramowanie wchodzące w skład Systemu PSeAP, do którego Wykonawca lub podmioty od niego zależne posiadają majątkowe prawa autorskie, umożliwiające rozwój i sprzedaż tego oprogramowania.
Oprogramowanie licencyjne, oprogramowanie licencjonowane	Oprogramowanie dostarczane w ramach niniejszego zamówienia, do którego Wykonawca ani podmioty od niego zależne nie mają majątkowych praw autorskich, umożliwiających rozwój i sprzedaż tego oprogramowania.

Infrastruktura Sprzętowa SeUI	Ogół sprzętu wraz z oprogramowaniem podstawowym na potrzeby SeUI, wg specyfikacji przedstawionej w niniejszym OPZ, wdrażany w ramach Projektu PSeAP.
Infrastruktura Sprzętowa SEOD	Ogół sprzętu wraz z oprogramowaniem podstawowym na potrzeby SEOD, wg specyfikacji przedstawionej w niniejszym OPZ, wdrażany w ramach Projektu PSeAP u Partnerów Projektu.
System e-Usług Internetowych, SeUI	Wdrażany w ramach Projektu PSeAP system informatyczny (oprogramowanie) obsługujący wszystkich Partnerów Projektu, zlokalizowany w Centrum Przetwarzania Danych PSeAP, posadowiony na Infrastrukturze Sprzętowej SeUI. SeUI składa się z następujących głównych elementów: <ul style="list-style-type: none"> <li>• System zarządzania infrastrukturą,</li> <li>• System monitorowania infrastruktury,</li> <li>• System zarządzania incydentami,</li> <li>• System Zarządzania Treścią (CMS) (Portal e-Usług oraz Podsystem do Zarządzania Siecią Infomatów),</li> <li>• Centralny Portal Internetowy wraz z podsystemami,</li> <li>• System wirtualizacji środowiska serwerów,</li> <li>• System backupu,</li> <li>• System optymalizacji dostępu.</li> </ul>
Elektroniczna Skrzynka Podawcza	Określana w specyfikacji niniejszym OPZ także jako „ESP”. Pod pojęciem ESP rozumie się środek komunikacji elektronicznej opisany w Rozporządzeniu Prezesa Rady Ministrów w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym z dnia 29 września 2005 r. (Dz.U. z 2005r., Nr 200, poz. 1651 z późn. zm.). ESP na potrzeby Projektu będzie realizowana przez Platformę ePUAP.
Użytkownik SEOD	Pracownik urzędu gminy/miasta lub starostwa powiatowego u Partnera Projektu, używający SEOD w ramach wykonywania swoich obowiązków służbowych.
Urząd	Urząd Marszałkowski Województwa Podkarpackiego lub urząd gminy/miasta, będącego Partnerem Projektu lub starostwo powiatu, będącego Partnerem Projektu.
Użytkownik SeUI	Pracownik dowolnego Partnera projektu, wykonująca czynności służbowe z wykorzystaniem SeUI lub inna osoba, której Partner

	zlecił wykonanie czynności na rzecz Partnera z wykorzystaniem SeUI.
JRWA	Jednolity Rzeczowy Wykaz Akt, system klasyfikacji dokumentacji przez administrację publiczną zgodny z Rozporządzeniem Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych z dnia 18 stycznia 2011 r. (Dz.U. z 2011 r. nr 14 poz. 67).
Lider Projektu	Województwo Podkarpackie – Partner Projektu PSeAP, pełniący wiodącą rolę w Projekcie.
Projekt, Projekt PSeAP	„PSeAP – Podkarpacki System e-Administracji Publicznej”, realizowany przez 160 Partnerów, w tym Lidera.
Partner Projektu	Partner biorący udział w Projekcie PSeAP, wskazany w Załączniku Nr 1 do OPZ
SEOD Zewnętrzny	System elektronicznego obiegu dokumentów, użytkowany przez Partnera Projektu, zakupiony poza Projektem PSeAP.
Aplikacja dziedzinowa	Aplikacja użytkowana przez Partnera Projektu przeznaczona do realizacji zadań statutowych przez JST, inna niż SEOD lub Aplikacja BIP (na przykład księgowość, podatki, kadry i płace).
BIP	Biuletyn Informacji Publicznej, prowadzony przez Partnerów Projektu zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r. nr 112, poz. 1198 z późn. zm.).
Aplikacja BIP	Aplikacja wykorzystywana przez Partnera do obsługi i publikowania BIP.
E-usługa	Usługa publiczna świadczona elektronicznie.
Formularz standardowy	Formularz e-usługi w Projekcie, jednakowy co do treści merytorycznej i wykorzystywany przez co najmniej dwóch Partnerów świadczących daną usługę publiczną.
Instancja szkoleniowa	Kopia oprogramowania aplikacyjnego przeznaczona do szkoleń użytkowników i administratorów, która działa niezależnie od instancji produkcyjnej, na odrębnej bazie danych, ale ma analogiczną konfigurację. Ze względów bezpieczeństwa w instancji szkoleniowej nie są przetwarzane rzeczywiste dokumenty i sprawy, lecz dokumenty i sprawy tworzone na potrzeby szkoleń; również struktura urzędu i uprawnień może być inna.

## 2.2 Definicje skrótów

Skrót	Definicja
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej
ePUAP2	Rozbudowa Elektronicznej Platformy Usług Administracji Publicznej
pl.ID	polska ID karta (elektroniczny dowód osobisty)
ZMOKU	Zintegrowany Moduł Obsługi Końcowego Użytkownika
BUSC	Baza Usług Stanu Cywilnego
PESEL2	Powszechny Elektroniczny System Ewidencji Ludności
CPD	Centrum Przetwarzania Danych PSeAP
PSeAP	Podkarpacki System e-Administracji Publicznej
SeUI	System e-Usług Internetowych
CPI	Centralny Portal Internetowy
SEOD	System Elektronicznego Obiegu Dokumentów
JST	Jednostka Samorządu Terytorialnego
JRWA	Jednolity Rzeczowy Wykaz Akt
PIAP	Publiczny Punkt Dostępu do Internetu (Public Internet Access Point)
SOA	Architektura zorientowana na usługi (ang. Service Oriented Architecture)
Web Services	Usługi sieciowe
CMS	System zarządzania treścią ( <a href="#">ang.</a> Content Management System)
LAN	sieć lokalna (ang. Local Area Network)
WAN	rozległa sieć komputerowa znajdująca się na obszarze wykraczającym poza jedno miasto (ang. Wide Area Network)
VPN	wirtualna sieć prywatna (ang. Virtual Private Network), umożliwia kompresję lub szyfrowanie danych przez co zwiększa poziom bezpieczeństwa przesyłanych danych

---

### 3 Przedmiot zamówienia

Przedmiotem zamówienia w ramach niniejszego postępowania są prace analityczne, projektowe, wdrożeniowe, dokumentacyjne, szkolenia oraz działania promocyjne związane ze stworzeniem Podkarpackiego Systemu e-Administracji Publicznej.

Powyższe zamówienie obejmuje w szczególności:

Zadania objęte niniejszym postępowaniem, które zostaną zlecone Wykonawcy systemu informatycznego o nazwie *PSeAP — Podkarpacki System e-Administracji Publicznej*, obejmują:

- I) Zaprojektowanie, wykonanie i wdrożenie Systemu Elektronicznego Obiegu Dokumentów (SEOD);
- II) Zaprojektowanie, wykonanie i wdrożenie Systemu e-Uслуг Internetowych (SeUI) Wdrożenie e-usług publicznych Partnerów Projektu w dostarczonym systemie informatycznym oraz na platformie ePUAP;
- III) Dostawa sprzętu sieciowego oraz zestawienie łączności w sieci rozległej w oparciu o udostępnione łącza;
- IV) Dostawa i uruchomienie serwerów dla JST;
- V) Dostawa i uruchomienie komputerów osobistych dla JST;
- VI) Dostawa i instalacja pakietów biurowych;
- VII) Dostawa i uruchomienie infomatów dla JST;
- VIII) Dostawa i uruchomienie urządzeń do przyjmowania dokumentów (urządzeń wielofunkcyjnych) dla JST;
- IX) Dostawa zestawów do składania podpisu cyfrowego dla JST;
- X) Dostawa i uruchomienie sprzętu dla Centrum Przetwarzania Danych PSeAP;
- XI) Dostawa i wdrożenie systemu monitorowania i administrowanie sprzętu oraz oprogramowania;
- XII) Konfiguracja wszystkich elementów systemu PSeAP (m.in. utworzenie użytkowników, nadanie uprawnień, konfiguracja hierarchii zasobów, etc.);
- XIII) Przeprowadzenie instruktażu dla użytkowników i administratorów systemu;
- XIV) Przeprowadzenie szkoleń;
- XV) Promocja Projektu.

## 4 Harmonogram realizacji

Etap	Zakres zadania	Maksymalny czas zakończenia (od podpisania umowy)*
I	1. Opracowanie Planu Realizacji Projektu, w tym procedur współpracy, procedur odbiorów, planu wdrożenia.	12 dni roboczych
	2. Opracowanie uszczegółowionej architektury systemu oraz planu rozmieszczenia i konfiguracji poszczególnych elementów i warstw oprogramowania SeUI	20 dni roboczych
II	1. Opracowanie projektu technicznego całego systemu PSeAP, w szczególności projektu integracji z platformą ePUAP. 2. Opracowanie projektu struktury, nawigacji, grafiki oraz wyszukiwarki dla Portalu CPI oraz Portalu e-Uслуг.	30 dni roboczych
III	1. Dostawa urządzeń aktywnych tj.: <ul style="list-style-type: none"> <li>• Dostawa i konfiguracja przełączników</li> <li>• Dostawa i konfiguracja urządzeń do zabezpieczenia przesyłu i gromadzenia danych</li> <li>• Dostawa urządzeń oraz licencji oprogramowania do zabezpieczenia brzegu sieci VPN</li> </ul>	3 miesiące
	2. Dostawa sprzętu informatycznego , w tym: <ul style="list-style-type: none"> <li>• Dostawa, konfiguracja i wdrożenie systemu antywirusowego</li> <li>• Wdrożenie podpisu cyfrowego</li> <li>• Dostawa i konfiguracja urządzeń serwerowych (serwery macierze) do CPD</li> <li>• Dostawa i konfiguracja oprogramowania systemowego</li> <li>• Dostawa urządzeń oraz licencji oprogramowania do systemu monitorowania sieci</li> <li>• Dostawa, instalacja i konfiguracja serwerów (partnerzy)</li> </ul>	3 miesiące

	<ul style="list-style-type: none"> <li>• Dostawa zestawów komputerowych oraz notebooków</li> <li>• Dostawa i instalacja oprogramowania biurowego</li> <li>• Dostawa zestawów wielofunkcyjnych</li> <li>• Dostawa i konfiguracja infomatów zewnętrznych i wewnętrznych</li> </ul>	
IV	<ol style="list-style-type: none"> <li>1. Wdrożenie wstępnej (pilotażowej) wersji CPI oraz Portalu e-Uслуг, przeprowadzenie testów użyteczności z użytkownikami.</li> <li>2. Przeprowadzenie pilotażu SEOD – wdrożenie w 10 JST.</li> <li>3. Opracowanie formularzy i kompletne wdrożenie (z uwzględnieniem wdrożenia na ePUAP) po 3 e-usług publicznych na poziomie co najmniej 3 dla każdego z 10 uczestników pilotażu, w tym co najmniej 5 e-usług na poziomie 4. Wdrożenie dla każdej z tych e-usług odpowiednich ścieżek obiegu w SEOD.</li> <li>4. Dostawa licencji na potrzeby pilotażowego wdrożenia SEOD, a także na potrzeby CPI i Portalu e-Uслуг.</li> <li>5. Opracowanie procedur backupu, procedur zgłaszania awarii, procedur aktualizacji oprogramowania, osobno dla elementów Systemu zlokalizowanych u Partnerów Projektu oraz w CPD</li> <li>6. Opracowanie rekomendacji w zakresie zmian w polityce bezpieczeństwa dla Partnerów Projektu.</li> <li>7. Opracowanie rekomendowanego wzoru zarządzenia w sprawie przyjęcia systemu EZD jako podstawowego trybu pracy w jednostkach.</li> </ol>	5 miesięcy
V	<ol style="list-style-type: none"> <li>1. Dopracowanie mechanizmów, struktury i wyglądu oraz opracowanie treści dla Portalu CPI oraz Portalu e-Uслуг.</li> <li>2. Produkcyjne wdrożenie SeUI, w tym dostawa pozostałego sprzętu i licencji.</li> <li>3. Wdrożenie e-usług poziomu 1 (objętych Projektem) u wszystkich Partnerów Projektu, którzy zaakceptują opisy usług i dostarczą niezbędne informacje do kart usług.</li> </ol>	12 miesięcy

	<p>4. Opracowanie po jednym formularzu standardowym dla wszystkich usług poziomu 2-4 objętych projektem i wdrożenie tych usług u wszystkich Partnerów, którzy zadeklarują świadczenie usługi w oparciu o formularz standardowy.</p> <p>5. Wdrożenie dodatkowych 20 formularzy (standardowych lub nie standardowych) oraz powiązanych e-usług poziomu 2-4 u Partnerów Projektu.</p> <p>6. Dostawa pozostałych licencji na potrzeby SEOD.</p> <p>7. Dostawa informatów</p> <p>8. Produkcyjne wdrożenie SEOD, w szczególności wprowadzenie konfiguracji, użytkowników, uprawnień oraz po 10 ścieżek obiegu u każdego z Partnerów.</p> <p>9. Wdrożenie wszystkich wymaganych mechanizmów integracyjnych.</p> <p>10. Opracowanie projektów zarządzeń.</p> <p>11. Przekazanie dokumentacji.</p> <p>12. Przeprowadzenie instruktażu stanowiskowego i szkoleń.</p>	
VI	<p>Na każdym z powyższych etapów Wykonawca jest zobowiązany do prowadzeni projektu zgodnie z zasadami realizacji projektów unijnych, w tym do dostarczenia tablic informacyjnych, tablic pamiątkowych i naklejek na dostarczony sprzęt i oprogramowanie.</p>	12 miesięcy



---

## **5 Wymagania ogólne dotyczące przedmiotu zamówienia**

### **5.1 Wymagania dotyczące bezpieczeństwa**

Rozwiązanie techniczne zastosowane w PSeAP muszą umożliwiać tworzenie kopii zapasowych (archiwizacja pełna i przyrostowa) danych. Zaoferowane rozwiązania muszą być zdolne do tworzenia kopii zapasowych (backupu) danych dokonywanych minimum raz dziennie. Musi umożliwiać wybór między archiwizacją pełną a przyrostową. Na podstawie kopii zapasowych musi być możliwe automatyczne odtworzenie systemu PSeAP wraz z danymi w dowolnym momencie.

Wykonawca jest zobowiązany przedstawić modele organizacji bezpieczeństwa w Projekcie PSeAP, tworzące systemy zarządzania bezpieczeństwem dostępu do informacji, w szczególności procedur nadzoru i raportowania w odniesieniu do bezpieczeństwa przechowywanych danych. Wykonawca musi także opracować procedury backupu dla elementów systemu zlokalizowanych centralnie oraz u poszczególnych Partnerów. Procedury te muszą pozwalać na sprawne odtworzenie systemu i muszą opierać się na rozwiązaniach do backupu dostarczonych w ramach zamówienia.

System musi zapewnić działania zgodnie z zasadami gwarantującymi taką eksploatację Infrastruktury, aby zapewnić bezpieczeństwo informacji rozumiane jako: poufność, integralność i dostępność, przy uwzględnieniu autentyczności, rozliczalności, niezaprzeczalności i niezawodności.

### **5.2 Wymagania dotyczące wydajności i pojemności**

Wykonawca zobowiązany jest do zagwarantowania odpowiedniej wydajności i pojemności Systemu w okresie 5 lat od dnia dokonania odbioru końcowego. Jeśli jakiś element systemu nie będzie spełniał wymagań w zakresie wydajności i pojemności, Wykonawca na własny koszt dostarczy, zainstaluje i skonfiguruje dodatkowe elementy sprzętu i oprogramowania niezbędne do zapewnienia właściwej wydajności i pojemności. Jeśli brak wystarczającej wydajności lub pojemności będzie spowodowany wadliwym projektem lub wykonaniem autorskiego oprogramowania Wykonawcy, Wykonawca obowiązany jest je poprawić.

Wydajność Systemu musi być dostosowana przez Wykonawcę do ilości przetwarzanych w Systemie danych, liczby użytkowników oraz liczby transakcji – przy zachowaniu zapasu zakładającego wzrost obciążenia systemu w przyszłości. Wykonawca powinien oszacować niezbędną wydajność i pojemność Systemu w oparciu o założenie, że Partnerzy Projektu wybiorą system EZD jako system podstawowy prowadzenia czynności kancelaryjnych, 95% potencjalnych interesantów będzie korzystało z Portalu e-Uслуг jako źródła informacji (i formularzy do wydruku). Liczba użytkowników systemu jest podana dla każdego Partnera w Załączniku nr 1 do OPZ. Ponadto należy założyć, że rozmiar załączanych do sprawy skanów dokumentów będzie odpowiadał średnio skanowi 3 stron A4 z rozdzielczością nie przekraczającą 150 dpi.

---

Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych testów wydajnościowych (w dowolnym czasie w trakcie okresu gwarancyjnego) osobiście lub przez firmę trzecią, w obu przypadkach przy udziale Wykonawcy. Wykonawca zobowiązany jest do uwzględnienia uwag i wprowadzenia niezbędnych poprawek do PSeAP.

Czas odpowiedzi systemu na następujące polecenia:

- a) zapisu pisma,
- b) wyszukania pisma po sygnaturze sprawy i odczytu pisma,
- c) zapis sprawy utworzonej na podstawie pisma (maksymalna wielkość pliku zawierającego pismo 2 MB),
- d) wyszukanie sprawy i przypisanych do niej pism (nie więcej niż 5 pism w danej sprawie).

nie może przekraczać 5 sekund (w środowisku SEOD tzn. bez innych uruchomionych usług i aplikacji) przy pełnym obciążeniu systemu (tzn. u Partnera pracuje w systemie tyle użytkowników ile wynika z przewidywanej liczby licencji wg załącznika nr 1 do OPZ).

### **5.3 Wymagania ogólne dotyczące wdrożenia**

Wdrożenie systemu PSeAP obejmuje:

- a) przeprowadzenie analizy przedwdrożeniowej;
- b) dostawy, instalację, konfigurację i uruchomienie sprzętu i oprogramowania we wskazanych przez Zamawiającego lokalizacjach;
- c) przeprowadzenie pilotażu oraz testów użyteczności;
- d) wdrożenie środowiska testowego i przeprowadzenie testów funkcjonalnych Systemu;
- e) konfigurację i uruchomienie systemu PSeAP jako całości oraz przeprowadzenie testów;
- f) przeprowadzenie instruktaży stanowiskowych.

#### **5.3.1 Analiza przedwdrożeniowa**

W ramach analizy przedwdrożeniowej Wykonawca zobowiązany jest do:

- a) powołania wspólnie z Zamawiającym Zespołu Roboczego;
- b) delegowania do pracy w Zespole Roboczym co najmniej trzech analityków do momentu zakończenia prac projektowych;
- c) opracowania i uzgodnienia z Zamawiającym lub upoważnionego przez niego Inżyniera Kontraktu Planu Realizacji Projektu obejmującego w szczególności:

- 
- procedury współpracy (m.in. sposób uzgadniania zawartości i układu formularzy elektronicznych oraz opisów usług, zakres, format i sposób przekazania przez Partnerów informacji niezbędnych do wdrożenia<sup>1</sup>),
  - plan wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązanie dla sytuacji kryzysowych wdrożenia,
  - plan testów systemu uwzględniających sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
  - sposób i propozycja terminów odbioru w podziale na każdego z partnerów,
  - listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu.
  - opis przypadków, w których projekt dopuszcza niedziałanie systemu.
- d) opracowanie planu rozmieszczenia urządzeń oraz architektury logicznej włącznie z zabezpieczeniem sieci LAN; opracowanie konfiguracji poszczególnych elementów i warstw oprogramowania SeUI na zwirtualizowanych serwerach oraz na fizycznych serwerach w UMWP;
- e) oszacowanie zapotrzebowania poszczególnych elementów na zasoby sprzętowe (wydajność, pojemność);
- f) opracowania uszczegółowionej architektury systemu oraz planu rozmieszczenia i konfiguracji poszczególnych elementów i warstw oprogramowania SeUI;
- g) opracowania projektu technicznego całego systemu PSeAP, w szczególności projektu integracji z platformą ePUAP oraz specyfikacji interfejsów zewnętrznych;
- h) opracowania projektu struktury, nawigacji, grafiki oraz wyszukiwarki dla Portalu CPI oraz Portalu e-Usług;
- i) opracowania projektu interfejsu komunikacyjnego i graficznego SEOD, który zostanie uzgodniony i uzyska aprobatę Zamawiającego;
- j) opracowania opisów usług oraz propozycji formularzy standardowych, które będą podstawą do uzgodnień, dokonanie niezbędnych uzgodnień z Partnerami zgodnie z procedurami wynikającymi z Planu Realizacji Projektu;
- k) opracowanie modelowego planu konfiguracji Systemu, z uwzględnieniem poszczególnych rodzajów Partnerów i ich specyficznych uwarunkowań.

---

<sup>1</sup>Wykonawca powinien uwzględnić, że Partnerzy będą mieli prawo udostępnić informacje w takiej formie (formacie, układzie), w jakiej je już posiadają, np. udostępniają na swoich stronach podmiotowych BIP.

---

### 5.3.2 Dostawa, instalacja i konfiguracja sprzętu i oprogramowania

Wykonawca dostarczy, zainstaluje i skonfiguruje sprzęt i oprogramowanie na potrzeby Systemu PSeAP. Dostarczony sprzęt i oprogramowanie powinny być wystarczające do prawidłowego działania produkcyjnej wersji Systemu PSeAP w zakładanym kształcie, jak również do prawidłowego działania instancji szkoleniowej Systemu (jedna instancja szkoleniowa SEUI i SEOD w CPD oraz po jednej instancji szkoleniowej SEOD u każdego Partnera, u którego będzie wdrażany SEOD) oraz instancji testowej Systemu (jedna instancja testowa SEUI i SEOD w CPD oraz instancje testowe SEOD u każdego z 10 Partnerów – uczestników pilotażu).

Proces dostawy, instalacji i konfiguracji obejmuje w szczególności:

W zakresie sprzętu:

- a) przekazanie do Zamawiającego najpóźniej na 30 dni przed rozpoczęciem dostaw szczegółowego harmonogramu dostaw, instalacji i konfiguracji sprzętu i oprogramowania w podziale na partnerów projektu. Harmonogram ten musi być zatwierdzony przez wszystkich partnerów, których dotyczyć będą dostawy.
- b) fizyczny montaż serwerów, macierzy, urządzeń do archiwizacji oraz pozostałych komponentów w tym sprzętu sieciowego w szafie RACK w lokalizacji wskazanej przez Zamawiającego,
- c) fizyczny montaż sprzętu w lokalizacjach wskazanych przez Zamawiającego,
- d) podłączenie sprzętu do najbliższego punktu styku z Internetem oraz siecią energetyczną i wszystkimi wymaganymi instalacjami teletechnicznymi.

W zakresie instalacji i konfiguracji oprogramowania:

- a) instalację, konfigurację i uruchomienie oprogramowania podstawowego wymaganego niniejszą specyfikacją oraz wszelkiego innego niezbędnego do prawidłowego funkcjonowania Systemu PSeAP na dostarczonym sprzęcie (wirtualizacja, systemy operacyjne, sterowniki, itp.),
- b) instalację, konfigurację i uruchomienie na dostarczonym sprzęcie dostarczonego oprogramowania aplikacyjnego SEOD i SeUI, w tym niezbędnego oprogramowania pomocniczego SEOD i SeUI.

Szczegółowe wymagania w zakresie wdrożenia sprzętu znajdują się w odpowiednich rozdziałach niniejszego OPZ.

### 5.3.3 Pilotaż

- I) Pilotaż Portalu e-Uслуг i Portalu CPI obejmie dostawę, instalację i konfigurację sprzętu na potrzeby pilotażu w Centrum Przetwarzania Danych, wdrożenie struktury tych Portalu, wybranych treści oraz integracji z Platformą ePUAP oraz SEOD (u 10 Partnerów – uczestników pilotażu). Zakres wdrożenia pilotażowego musi być wystarczający, aby zweryfikować użyteczność tych Portalu (czytelność i łatwość dotarcia do informacji, sposób działania wyszukiwarki e-usług, ergonomię funkcji związanych z pracą grupową oraz tworzeniem

- 
- i publikacją e-usług). W szczególności wymaga się wykorzystania Portalu CPI do uzgadniania formularzy standardowych oraz kart e-usług co najmniej dla e-usług będących przedmiotem pilotażu.
- II) W ramach pilotażu elementów SeUI Wykonawca przeszkoli administratorów Partnerów uczestniczących we wdrożeniu oraz 3 administratorów Lidera z wykorzystania wdrożonych w pilotażu narzędzi SEUI. Ponadto przeprowadzone zostaną testy, w tym testy podatności i testy użyteczności z udziałem administratorów oraz potencjalnych użytkowników.
- III) Pilotaż systemu SEOD będzie przeprowadzony u 10 Partnerów, wskazanych przez Zamawiającego na etapie analizy przedwdrożeniowej. Dla tych Partnerów będą również wdrożone odpowiednie elementy na pilotażowej wersji SeUI (w szczególności – uprawnienia oraz integracja między SEOD a SeUI).
- IV) Pilotaż obejmie opracowanie formularzy i kompletne wdrożenie (z uwzględnieniem wdrożenia na ePUAP) po 3 e-usług publicznych na poziomie co najmniej 3 dla każdego z 10 uczestników pilotażu, w tym co najmniej 5 e-usług na poziomie 4. Wykonawca wdroży dla każdej z tych e-usług odpowiednie ścieżki obiegu dokumentów w SEOD.
- V) W zakres wdrożenia pilotażowego u Partnera wchodzić będą następujące zadania:
- a) Uruchomienie funkcji sieci rozległej pomiędzy lokalizacjami, w oparciu o łącza eksploatowane przez Partnera.
  - b) Instalacja sprzętu aktywnego w sieciach LAN.
  - c) Dostawa i uruchomienie zestawów serwerowych.
  - d) Dostawa i uruchomienie komputerów osobistych.
  - e) Dostawa i uruchomienie infomatów.
  - f) Dostawa i uruchomienie zestawów do Biura Obsługi Klientów.
  - g) Dostawa i uruchomienie zestawów do składania podpisu cyfrowego.
  - h) Dostawa i wdrożenie SEOD u 10 Partnerów, wraz z instruktażami stanowiskowymi.
  - i) Przeprowadzenie testów, w tym testów dostępności testów użyteczności interfejsu SEOD.
- VI) W wyniku pilotażu wykonawca zobowiązany jest uwzględnić ewentualne uwagi do procedur, konfiguracji, wydajności oraz innych aspektów działania Systemu i zaktualizować odpowiednio dokumenty projektowe, w szczególności wypracowane na etapie analizy przedwdrożeniowej.
- VII) W ramach pilotażu będą wykonane testy podatności, w tym testy wydajności, dostępności i bezpieczeństwa pilotażowego SeUI oraz SEOD. Będą one przeprowadzone przy udziale pracowników jednostek uczestniczących w pilotażu w oparciu o testową bazę danych, symulującą stopień zapełnienia bazy danych po 5 latach użytkowania systemu PSeAP jako systemu EZD.
- VIII) Podstawą do odbioru wdrożenia pilotażowego będą następujące protokoły:
- a) protokół odbioru pilotażowego wdrożenia Portalu e-Usług oraz Portalu CPI (wraz z wynikami testów użyteczności) podpisany przez Zamawiającego;
-

- b) komplet protokołów podpisanych przez Partnerów i zatwierdzonych przez Zamawiającego – w zakresie części pilotażu przypadających na poszczególnych Partnerów;
- c) protokół odbioru zaktualizowanych dokumentów projektowych, które wymagały zmian w wyniku pilotażu.

Odbiór wdrożenia pilotażowego nie jest równoznaczny z odbiorem wdrożenia produkcyjnego.

W przypadku wystąpienia błędów krytycznych lub poważnych pilotaż nie może zostać odebrany do czasu ich usunięcia.

Wyniki przeprowadzonych testów oraz wnioski sformułowane na etapie pilotażu zostaną uwzględnione i posłużą do przygotowania ostatecznej wersji i produkcyjnego wdrożenia Systemu PSeAP.

#### 5.3.4 Środowisko testowe i testy funkcjonalne Systemu

	Minimalne wymagania dotyczące Wdrożenia środowiska testowego
	<b>Zasady ogólne</b>
WT SEUI 1	Przez „środowisko testowe” rozumie się tutaj normalnie działające oprogramowanie SEOD i SeUI, które nie jest zaangażowane w świadczenie usług Systemu w ramach rozwiązania PSeAP.  Środowisko testowe musi zawierać dane testowe umożliwiające przeprowadzanie scenariuszy testowych.  Środowisko testowe musi korzystać ze wsparcia systemów zewnętrznych, emulujących zachowanie zewnętrznych źródeł danych, z którymi System ma docelowo współpracować, w szczególności z testowej wersji Platformy ePUAP.
WT SEUI 2	Przed wdrożeniem środowiska testowego, Wykonawca musi zainstalować oraz uruchomić produkcyjnie platformę sprzętową Systemu w siedzibie UMWP oraz platformę sprzętową SEOD u dziesięciu Partnerów, u których będzie się znajdowało środowisko testowe SEOD.
WT SEUI 3	Wykonawca musi zainstalować oraz uruchomić środowisko testowe SeUI na produkcyjnej platformie sprzętowej w CPD, zaś środowisko testowe SEOD – na produkcyjnej platformie sprzętowej u dziesięciu Partnerów Projektu, wskazanych przez Zamawiającego oraz dodatkowo jedną instancję testową SEOD w CPD.
	<b>Konfiguracja środowiska testowego</b>
WT SEUI 4	Na etapie konfiguracji środowiska testowego, Wykonawca musi wprowadzić do

	<p>Systemu ustawienia konfiguracyjne oraz dane niezbędne do poprawnego działania Systemu podczas fazy testów funkcjonalnych, w tym co najmniej:</p> <p>A) Konta i role użytkowników Systemu.</p> <p>B) Predefiniowane formularze elektroniczne.</p>
WT SEUI 5	Na etapie konfiguracji środowiska testowego, Wykonawca musi zapewnić usługi zewnętrzne, emulujące zachowanie zewnętrznych źródeł danych, z którymi SeUI i SEOD mają docelowo współpracować.
WT SEUI 6	Od momentu rozpoczęcia testów akceptacyjnych do momentu ostatecznego odbioru Systemu środowisko testowe musi być skonfigurowane identycznie skonfigurowane jak środowisko produkcyjne.
	<b>Testy funkcjonalne Systemu</b>
WT SEUI 7	Funkcjonalne testy akceptacyjne Systemu muszą być zrealizowane w środowisku testowym. Testy te muszą obejmować w szczególności testy integracyjne oraz regresyjne, w przypadku zmian oprogramowania.
WT SEUI 8	Podczas akceptacyjnych testów funkcjonalnych, Zamawiający zweryfikuje zgodność dostarczonego Systemu z obowiązującą Wykonawcę specyfikacją funkcjonalną.
WT SEUI 9	Pomyślne zakończenie akceptacyjnych testów funkcjonalnych będzie równoznaczne z uzyskaniem przez Wykonawcę potwierdzenia odbioru funkcjonalnego Systemu.

### 5.3.5 Konfiguracja i produkcyjne uruchomienie systemu PSeAP

W ramach konfiguracji i produkcyjnego uruchomienia Systemu PSeAP, Wykonawca:

- I) wdroży interfejsy komunikacyjne między elementami składającymi się na system,
- II) wdroży system uprawnień,
- III) wdroży struktury organizacyjne jednostek i użytkowników, nadając im odpowiednie uprawnienia w SEOD i SeUI,
- IV) przygotuje interfejsy integracyjne do systemów zewnętrznych (w uzgodnionym standardowym formacie), w tym BIP, zewnętrzne systemy SEOD Partnerów, a dla czterech Partnerów Projektu korzystających obecnie z systemu SEOD (gmina miejska Lubaczów, gmina Jasło, powiat przemyski, gmina Jedlicze) dokona migracji wszystkich otwartych spraw do nowego systemu,

- V) wykonana pełną integrację z systemem ePUAP;
- VI) do momentu oddania systemu do eksploatacji produkcyjnej wdroży 420 różnych e-usług publicznych (opisanych w rozdziałach 7.1 i 7.2), usługi te muszą być unikatowe w stosunku do zamieszczonych na ePUAP w dniu odbioru,
- VII) wdroży instancję szkoleniową SEOD (u każdego z Partnerów) i SeUI (u Lidera),
- VIII) opracuje szczegółowy plan testów pozafunkcyjnych Systemu w uzgodnieniu z Zamawiającym i przeprowadzi te testy pod nadzorem Zamawiającego. Testy niefunkcjonalne obejmą w szczególności: testy wydajnościowe, przeciążeniowe i obciążeniowe, odtwarzania po awarii, testy konfiguracji, testy bezpieczeństwa, testy integracyjne i regresyjne. Będą one wykonane na produkcyjnej instancji Systemu przed jej ostatecznym odbiorem i przekazaniem do eksploatacji. Wybrane testy, wymagające zasilania systemu dużymi zbiorami danych testowych, mogą być przeprowadzone na środowisku testowym. Warunkiem odbioru systemu jest pozytywne przejście wszystkich testów.

Szczegółowe wymagania, dotyczące procesu wdrożenia SEUI i SEOD są opisane w odpowiednich rozdziałach niniejszego OPZ.

### 5.3.6 Instruktaż stanowiskowy

Wykonawca obowiązany jest zapewnić sprzęt komputerowy na potrzeby instruktaży stanowiskowych dla użytkowników SEOD oraz administratorów.

Instruktaże stanowiskowe odbywać się będą w wytypowanych siedzibach partnerów (min. 1 w każdym z powiatów), w grupach maksymalnie 10-osobowych.

Jeden dzień instruktażu obejmować będzie nie więcej niż 7 jednostek 45-minutowych.

#### 5.3.6.1 Instruktaż stanowiskowy dla administratorów w zakresie SeUI i SEOD

Wymaganie	Wymagania szczegółowe dla przeprowadzenia instruktażu stanowiskowego
IS SEUI 1	<p>Instruktaż stanowiskowy dla roli administratora lokalnego obejmuje:</p> <ul style="list-style-type: none"> <li>A) funkcjonalność SEOD w odniesieniu do poszczególnych zadań administracyjnych związanych z SEOD,</li> <li>B) funkcjonalność poszczególnych narzędzi SeUI w odniesieniu do zadań administratorów lokalnych,</li> <li>C) inne istotne aspekty systemu PSeAP, w szczególności dotyczące zapewnienia bezpieczeństwa, niezawodności i wydajności lokalnie zainstalowanych komponentów Systemu PSeAP,</li> <li>D) proces definiowania i wdrażania nowych e-usług, w tym niezbędnych formularzy i konfiguracji, z uwzględnieniem wszystkich czynności wykonywanych w SEOD, SeUI oraz na Platformie ePUAP,</li> </ul>



	<p>E) tworzenie i modyfikację formularzy elektronicznych w dostarczonym edytorze formularzy,</p> <p>F) proces definiowania i wdrażania nowych ścieżek obiegu dokumentów, w tym wszelkich niezbędnych konfiguracji, formularzy, szablonów dokumentów, z uwzględnieniem wszystkich czynności wykonywanych w SEOD, SeUI oraz na Platformie ePUAP,</p> <p>G) proces definiowania i wdrażania integracji z systemami dziedzinowymi oraz z systemami BIP i systemami centralnymi,</p> <p>H) ideę reużywalności oraz praktyczny zakres i możliwości wykorzystania rozwiązań opracowanych przez innych,</p> <p>I) techniczne aspekty oraz procedury aktualizacji oprogramowania i jego konfiguracji,</p> <p>J) procedury związane ze zgłaszaniem awarii, korzystaniem z pomocy w okresie asysty,</p> <p>K) procedury postępowania w sytuacjach awaryjnych,</p> <p>L) procedury backupu SEOD.</p> <p>Punkty A, B, D, E, F i L muszą być poparte praktycznymi ćwiczeniami (instruktaż praktyczny).</p> <p>Instruktaż stanowiskowy będzie miał wymiar co najmniej 20 jednostek 45-minutowych. Liczba administratorów biorących udział w instruktażu od każdego Partnera podana została w załączniku nr 2 do OPZ.</p> <p>Dopuszcza się połączenie instruktażu udzielanego osobiście z instruktażem wykorzystującym platformę e-learningową, pod warunkiem, że co najmniej 10 jednostek instruktażu w tym cztery ostatnie dla każdego administratora, odbędzie się podczas osobistego spotkania.</p>
IS SEUI 2	<p>Instruktaż stanowiskowy dla roli administratora globalnego obejmie wszystkie elementy przewidziane dla administratorów lokalnych oraz:</p> <p>A) funkcjonalność poszczególnych narzędzi SeUI w odniesieniu do zadań administratorów centralnych,</p> <p>B) istotne aspekty systemu PSeAP, w szczególności dotyczące zapewnienia bezpieczeństwa, niezawodności i wydajności,</p> <p>C) proces dodawania nowych użytkowników i zarządzania użytkownikami SeUI,</p> <p>D) proces aktualizacji oraz zarządzania aktualizacjami i konfiguracjami,</p> <p>E) procedura wdrażania nowych wersji oprogramowania z uwzględnieniem wersji testowej i szkoleniowej,</p> <p>F) zasady, zakres i szczegóły techniczne integracji z Platformą ePUAP oraz integracji pomiędzy poszczególnymi komponentami Systemu PSeAP,</p>

	<p>a także funkcjonalności Single Sign-On,</p> <p>G) procedury związane ze zgłaszaniem awarii, korzystaniem z pomocy w okresie asysty dla SeUI;</p> <p>H) procedury postępowania w sytuacjach awaryjnych dla SeUI,</p> <p>I) procedury backupu SeUI.</p> <p>Punkty A, E, H, I muszą być poparte praktycznymi ćwiczeniami (instruktaż praktyczny).</p> <p>Instruktaż stanowiskowy będzie miał wymiar co najmniej 40 jednostek 45-minutowych obejmie 5 administratorów.</p> <p>Dopuszcza się wykorzystanie do instruktażu platformy e-learningowej, pod warunkiem, że co najmniej 24 jednostki 45-minutowe instruktażu w tym cztery ostatnie dla każdego administratora, odbędą się podczas osobistego spotkania.</p>
IS SEUI 3	Program każdego z powyższych Instruktaży stanowiskowych musi umożliwiać osobie szkolonej opanowanie praktycznej umiejętności korzystania z funkcji Systemu przydatnych podczas normalnej pracy w roli, której dotyczy instruktaż.
IS SEUI 4	<p>Na potrzeby Instruktaży stanowiskowych praktycznych, Wykonawca musi zapewnić:</p> <p>A) odpowiednio przygotowany system przeprowadzenia instruktaży,</p> <p>B) oddzielny terminal komputerowy z pełnym dostępem do systemu szkoleniowego dla każdego uczestnika instruktażu stanowiskowego.</p>
IS SEUI 5	Każdy Instruktaż stanowiskowy praktyczny musi zostać zakończony egzaminem dwustopniowym, składającym się z testu sprawdzającego poziom wiedzy uczestników instruktażu oraz z egzaminu praktycznego, sprawdzającego ich umiejętność posługiwania się Systemem w zakresie obejmującym co najmniej przeciwiczone uprzednio przypadki użycia SeUI.
IS SEUI 6	Programy Instruktaży stanowiskowych z wykorzystaniem platformy e-learningowej muszą zawierać interaktywne symulacje, wymagające od osoby biorącej udział w instruktażu przeprowadzenia na makiecie interfejsu użytkownika Systemu operacji z zakresu podstawowych przypadków użycia Systemu, występujących podczas normalnej pracy w roli, której dotyczy odnośne Instruktażu stanowiskowego.
IS SEUI 7	Każdy z Instruktaży stanowiskowych teoretycznych musi zostać zakończony egzaminem testowym, sprawdzającym poziom wiedzy uczestników po odbyciu instruktażu.
IS SEUI 8	Każdy uczestnik instruktażu musi otrzymać dostęp do wersji elektronicznej materiałów szkoleniowych użytych podczas tego instruktażu.
IS SEUI 9	Przeprowadzenie wszystkich Instruktaży stanowiskowych przewidzianych w związku z wdrożeniem SeUI i SEOD stanowi warunek konieczny do zamknięcia

wdrożenia Projektu.

### 5.3.6.2 Instruktaż stanowiskowy dla pozostałych użytkowników SEOD

Wymaganie	Minimalne wymagania dotyczące Instruktażu stanowiskowego Użytkowników Systemu
	<b>Ogólne</b>
IS SEOD 1	Program instruktażu stanowiskowego dla użytkowników Systemu musi zakładać u osób szkolonych następujący poziom ogólnych kompetencji IT, tzn. umiejętność korzystania z edytora tekstu na poziomie podstawowym, umiejętność wykonywania operacji na folderach i plikach, korzystania z przeglądarki i poczty elektronicznej, komunikatora.
IS SEOD 2	<p>Program instruktażu stanowiskowego dla kluczowych użytkowników Systemu musi umożliwiać osobom biorącym udział w instruktażu opanowanie praktycznej umiejętności korzystania z wszystkich tych funkcji SEOD, którymi osoby te będą następnie posługiwać się w trakcie normalnej pracy z Systemem. Ponadto powinien przybliżyć im podstawowe pojęcia i zasady pracy z dokumentami elektronicznymi w urzędzie w takim zakresie, w jakim jest to niezbędne dla zrozumienia zasad działania systemu. Wymiar instruktażu wynosi 7 jednostek 45-minutowych. Liczba kluczowych użytkowników w podziale na każdego z partnerów podana zawarta została w załączniku nr 2 do OPZ.</p> <p>Odrębnie powinny zostać opracowane i przeprowadzone moduły dodatkowe instruktażu:</p> <ul style="list-style-type: none"> <li>• instruktaż dla archiwisty (dodatkowe 8 godzin),</li> <li>• instruktaż dla kadry zarządczej jst (dodatkowe 4 godziny).</li> </ul>
IS SEOD 3	Pozostali użytkownicy Systemu powinni zostać objęci instruktażami stanowiskowymi odbywającymi się z wykorzystaniem platformy e-learningowej. Liczba pozostałych użytkowników w podziale na każdego z partnerów podana zawarta została w załączniku nr 2 do OPZ.
IS SEOD 4	Zmodyfikowana wersja instruktażu w wymiarze 8 jednostek 45-minutowych powinna objąć administratorów lokalnych (poszerzona o problemy, błędy i zadania nietypowe, ale zakładająca wyższy poziom kompetencji ICT).
IS SEOD 5	<p>Program instruktażu stanowiskowego dla użytkowników Systemu musi obejmować co najmniej następujące zagadnienia:</p> <p>A) ogólne wiadomości dotyczące struktury Systemu, widoków interfejsu</p>

	<p>użytkownika Systemu oraz podstawowych typów występujących w SEOD obiektów; rejestracja korespondencji i spraw,</p> <p>B) dekretowanie dokumentów elektronicznych;</p> <p>C) praca z Ewidencją Klientów Urzędu;</p> <p>D) praca ze ścieżkami obiegu dokumentów,</p> <p>E) korzystanie z funkcji wyszukiwania i filtrowania;</p> <p>F) korzystanie z narzędzi pracy grupowej;</p> <p>G) przyjmowanie i wysyłanie dokumentów elektronicznych.</p>
IS SEOD 6	<p>Instruktaż stanowiskowy dla użytkowników Systemu musi zawierać interaktywne symulacje, wymagające od osoby szkolonej przeprowadzenia określonych operacji na makiecie interfejsu użytkownika Systemu.</p> <p>A) Wykonawca musi zapewnić symulacje, odpowiadające co najmniej dwudziestu najważniejszym przypadkom użycia SEOD, występującym podczas normalnej pracy użytkownika z Systemem.</p> <p>B) W charakterze w/w symulacji, Wykonawca może przeprowadzić z osobami biorącymi udział w instruktażu odpowiednie ćwiczenia praktyczne na systemie szkoleniowym.</p> <p>C) Wykonawca musi zapewnić wszystkim użytkownikom Systemu dostęp do w/w symulacji także po zakończeniu instruktażu stanowiskowego.</p>
IS SEOD 7	<p>Instruktaż stanowiskowy dla kluczowych użytkowników Systemu musi być zakończony egzaminem testowym, sprawdzającym poziom wiedzy uczestników po zakończeniu instruktażu stanowiskowego i wydaniem certyfikatu.</p>

## 5.4 Wymagania prawne

Wykonawca powinien stosować się do następujących aktów prawnych:

- SEOD musi być zgodny z przepisami prawa, obowiązującymi na dzień odbioru systemu.
- Elektroniczny Obieg Dokumentów musi pełnić funkcję i spełniać wszystkie warunki określone dla systemu EZD w Rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
- SEOD musi być zgodny w szczególności z następującymi przepisami prawa:
  - I) USTAWY:
    - a) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. Nr 64, poz. 565 z późn. zm.).

- 
- b) Ustawa z dnia 14 czerwca 1960 Kodeks Postępowania Administracyjnego (Dz.U. z 2000 r. Nr 98, poz. 1071 z późn. zm.).
  - c) Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r. Nr 112, poz. 1198 z późn. zm.).
  - d) Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2001 r. Nr 130, poz. 1450 z późn. zm.).
  - e) Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. Nr 144, poz. 1204 z późn. zm.).
  - f) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
  - g) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182 poz. 1228).
  - h) Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. z 2002 r. Nr 126 poz. 1068 z późn. zm.)
  - i) Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. Nr 128 poz. 1402 z późn. zm.
  - j) Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. z 1964 r. Nr 16 poz. 93 z późn. zm.)
  - k) Ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz.U. z 2011 r. Nr 197, poz. 1172).
  - l) Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz.U. z 2005 r. Nr 8, poz. 60 z późn. zm.).
  - m) Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz.U. z 2010 r. Nr 193 poz. 1287) i przepisy wykonawcze.
  - n) Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. 2010 nr 113 poz. 759 z późn. zm.).
  - o) Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2011 r. Nr 123 poz. 698).

## II) ROZPORZĄDZENIA:

- a) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 marca 2012 r. w sprawie wzoru i sposobu prowadzenia metryki sprawy (Dz.U. z 2012 r. poz. 250).
- b) Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14, poz. 67 z późn. zm.).

- 
- c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz.U. z 2011 r. Nr 93, poz. 545).
  - d) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz.U. z 2011 r. Nr 93, poz. 546).
  - e) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zasad potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz.U. z 2011 r. Nr 93, poz. 547).
  - f) Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2011 r. Nr 206, poz. 1216).
  - g) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).
  - h) Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. z 2002 r. Nr 128, poz. 1094).
  - i) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych. (Dz.U. z 2006 r. Nr 206, poz. 1519).
  - j) Rozporządzenie Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków (Dz.U. z 2002 r. Nr 5, poz. 46).
  - k) Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz.U. z 2005 r. Nr 205 poz. 1692).
  - l) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r. Nr 206 poz. 1518).
-

- 
- m) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz.U. z 2006 r. Nr 206 poz. 1517).
  - n) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. z 2007 r. Nr 10 poz. 68).
  - o) Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz.U. z 2005 r. Nr 217 poz. 1836).
  - p) Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz.U. z 2002 r. Nr 167 poz. 1375).
  - q) Rozporządzenie Prezesa Rady Ministrów z dnia 27 grudnia 2011 r. w sprawie wymagań technicznych dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne, dzienników urzędowych wydawanych w postaci elektronicznej oraz środków komunikacji elektronicznej i informatycznych nośników danych (Dz.U. z 2011r. Nr 289, poz. 1699).
  - r) Rozporządzenie Prezesa Rady Ministrów z dnia 3 października 2011 r. w sprawie określenia wzoru graficznego winiety dzienników urzędowych oraz pierwszej i ostatniej strony Dziennika Urzędowego Rzeczypospolitej Polskiej „Monitor Polski B”, a także wzoru okładek i strony tytułowej załączników do tego dziennika urzędowego (Dz.U. z 2011 r. Nr 214, poz. 1269).
  - s) Rozporządzeniem Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz.U. z 2002 r. Nr 100, poz.908).
  - t) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z dnia 16 maja 2012 r. poz. 526).

## **5.5 Równoważność rozwiązań**

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie



---

całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym.

W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację dostarczoną przez Wykonawcę potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

## **5.6 Wymagania w zakresie dokumentacji**

Wykonawca dostarczy dokumentację dla wszystkich elementów systemu PSeAP. Wymagane są w szczególności:

- I) Podręcznik użytkownika SEOD, opisujący funkcjonalność w odniesieniu do zadań wykonywanych przez użytkowników końcowych SEOD;
- II) Podręcznik administratora lokalnego, opisujący:
  - a) funkcjonalność SEOD w odniesieniu do poszczególnych zadań administracyjnych związanych z SEOD,
  - b) funkcjonalność poszczególnych narzędzi SeUI w odniesieniu do zadań administratorów lokalnych,
  - c) inne istotne aspekty systemu PSeAP, w szczególności informacje i instrukcje dotyczące zapewnienia bezpieczeństwa, niezawodności i wydajności lokalnie zainstalowanych komponentów Systemu PSeAP,
  - d) szczegółowy opis (od strony technicznej i organizacyjnej) procesu definiowania i wdrażania nowych e-usług, w tym niezbędnych formularzy i konfiguracji, z uwzględnieniem wszystkich czynności wykonywanych w SEOD, SeUI oraz na Platformie ePUAP,
  - e) szczegółowy opis (od strony technicznej i organizacyjnej) procesu definiowania i wdrażania nowych ścieżek obiegu dokumentów, w tym wszelkich niezbędnych konfiguracji, formularzy, szablonów dokumentów, z uwzględnieniem wszystkich czynności wykonywanych w SEOD, SeUI oraz na Platformie ePUAP,
  - f) szczegółowy opis (od strony technicznej i organizacyjnej) procesu definiowania i wdrażania integracji z systemami dziedzinowymi oraz z systemami BIP,



- g) ideę reużywalności oraz praktyczny zakres i możliwości wykorzystania rozwiązań opracowanych przez innych,
- h) techniczne aspekty oraz procedury aktualizacji oprogramowania i jego konfiguracji,
- i) procedury związane ze zgłaszaniem awarii, korzystaniem z pomocy w okresie asysty,
- j) procedury postępowania w sytuacjach awaryjnych,
- k) procedury backupu.

III) Podręcznik administratora centralnego, opisujący:

- a) elementy zawarte w podręczniku administratora lokalnego, w takim zakresie, jak będą one przydatne w pracy administratorów centralnych,
- b) funkcjonalność poszczególnych narzędzi SeUI w odniesieniu do zadań administratorów centralnych,
- c) istotne aspekty systemu PSeAP, w szczególności informacje i instrukcje dotyczące zapewnienia bezpieczeństwa, niezawodności i wydajności,
- d) szczegółowy opis (od strony technicznej i organizacyjnej) procesu dodawania nowych użytkowników i zarządzania użytkownikami SeUI,
- e) szczegółowy opis (od strony technicznej i organizacyjnej) procesu aktualizacji oraz zarządzania aktualizacjami i konfiguracjami,
- f) szczegółowy opis i procedura wdrażania nowych wersji oprogramowania z uwzględnieniem wersji testowej i szkoleniowej,
- g) szczegółowy opis integracji z Platformą ePUAP oraz interfejsów pomiędzy poszczególnymi komponentami Systemu PSeAP, a także funkcjonalności Single Sign-On,
- h) procedury związane ze zgłaszaniem awarii, korzystaniem z pomocy w okresie asysty;
- i) procedury postępowania w sytuacjach awaryjnych,
- j) procedury backupu.

IV) Podręcznik integratora, zawierający specyfikacje interfejsów oraz objaśnienia i opisy, umożliwiające dostosowanie systemów zewnętrznych do współpracy z systemem PSeAP.

V) Dokumentację producenta dla oprogramowania licencyjnego, w tym także umowa licencyjna, warunki gwarancji.

Elektroniczne wersje dokumentacji powinny być dostępne w postaci .pdf oraz zestawu powiązanych hiperłączami stron internetowych.

Liczba i forma dokumentacji:

- I) dokumentacja użytkownika końcowego: dla każdej lokalizacji Partnera co najmniej 1 egz. papierowy i 1 płyta CD lub DVD,
- II) dokumentacja administratora lokalnego: dla każdego Partnera co najmniej 1 egz. papierowy i 1 płyta CD lub DVD,
- III) dokumentacja administratora centralnego: co najmniej 5 egzemplarzy papierowych i 5 na płycie CD lub DVD,

---

IV) dokumentacja integratora: co najmniej po 1 egzemplarzu papierowym i 1 płycie CD lub DVD dla każdego Partnera, dodatkowo online w Portalu e-Uслуг,

V) dokumentacja producenta: dołączona do każdej licencji.

Ponadto dla oprogramowania autorskiego wymagane jest zdeponowanie wraz z kodami źródłowymi pełnej dokumentacji programisty, obejmującej co najmniej specyfikacje interfejsów komponentów wraz z określeniem poszczególnych funkcji, model obiektowy, model bazy danych wraz z opisem znaczenia poszczególnych wartości, dokumentację poszczególnych klas wygenerowaną automatycznie.

W okresie gwarancji Wykonawca obowiązany jest aktualizować i uzupełniać dokumentację zgodnie z wdrażanymi zmianami w oprogramowaniu. Aktualizacja polega na zamieszczeniu nowych wersji dokumentacji na Portalu CPI oraz errat do wydruku do dołączenia do wersji papierowej. W przypadku stwierdzenia przez Zamawiającego błędów lub braków w dokumentacji w okresie gwarancji, Wykonawca obowiązany jest uzupełnić i poprawić dokumentację.

Ponadto dostarczona przez Wykonawcę dokumentacja musi być zgodna z dokumentem projektowym „Wymagania dla Dokumentacji Technicznej Produktów”, załączonym do niniejszego OPZ.

### **5.7 Inne wymagania ogólne**

Wymaga się, aby wszystkie elementy SEOD i SeUI posiadały interfejs użytkownika w języku polskim. W języku polskim muszą być również wyświetlane wszystkie komunikaty przekazywane przez SEOD i SeUI, włącznie z komunikatami o błędach (z wyłączeniem opisu błędu przekazywanego z poziomu oprogramowania podstawowego i pomocniczego). Wymaga się, aby komunikaty o błędach przekazywane przez SEOD i SeUI zawierały opis błędu.

Partnerzy Projektu aktualnie wykorzystują w swojej pracy określone oprogramowanie, wyspecyfikowane w załączniku Nr 2 do niniejszego OPZ Zakres i wymiar instruktażu stanowiskowego oraz szkoleń musi uwzględnić różnice pomiędzy oprogramowaniem aktualnie użytkowanym a oferowanym, tzn. w wyniku wdrożenia użytkownicy muszą posiadać umiejętność obsługi zaoferowanego oprogramowania w stopniu wystarczającym do realizacji swoich zadań.

---

## 6 Architektura i Główne Komponenty

SEOD wraz z Portalem e-Uслуг oraz podsystemem formularzy elektronicznych ma pełnić z perspektywy Partnerów Projektu następujące główne role:

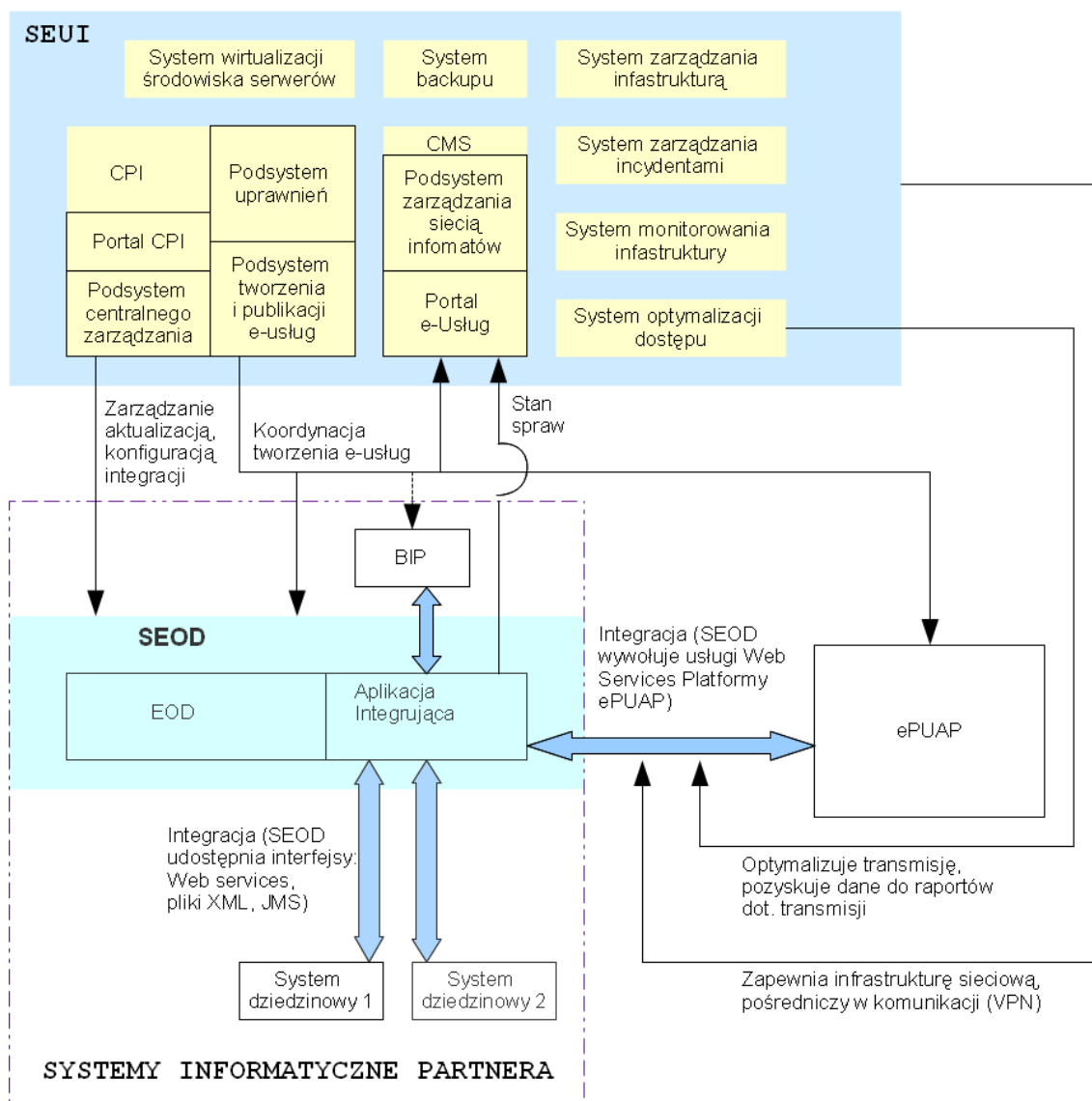
- platforma do przechowywania i obiegu dokumentów oraz realizacji czynności kancelaryjnych w formie elektronicznej (system SEOD będzie pełnił docelowo funkcję EZD w rozumieniu Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67);
- platforma do wspierania procesów realizowanych w Jednostkach Samorządu Terytorialnego (automatyzacja przepływu pracy poprzez ścieżki obiegu skonfigurowane w ramach SEOD, a także możliwość integracji z systemami dziedzinowymi z wykorzystaniem interfejsów wymiany danych dostępnych w ramach SEOD);
- platforma świadczenia e-usług publicznych online (Portal e-Uслуг jako platforma informacyjna, integracja z ePUAP w zakresie przyjmowania i doręczania dokumentów);
- platforma do grupowego tworzenia i zarządzania standardowymi wzorami dokumentów, formularzami elektronicznymi na potrzeby publikacji online oraz wykorzystania w procesach przepływu pracy w SEOD przez Partnerów (podsystem tworzenia i publikacji e-usług).

Architekturę Systemu przedstawia Rysunek 1 (dla Partnerów, którzy będą wdrażali SEOD w ramach Projektu). Dotyczy on powiązań funkcjonalnych pomiędzy systemami SeUI i SEOD oraz pokazuje interfejsy integracyjne z systemami zewnętrznymi. Należy pamiętać, że w Projekcie oprócz przedstawionego na poniższym rysunku dedykowanego oprogramowania występuje także poziom infrastrukturalny, obejmujący sprzęt i sieć teleinformatyczną w poszczególnych jej warstwach.

Użyte na diagramach oznaczenia należy interpretować w sposób następujący:

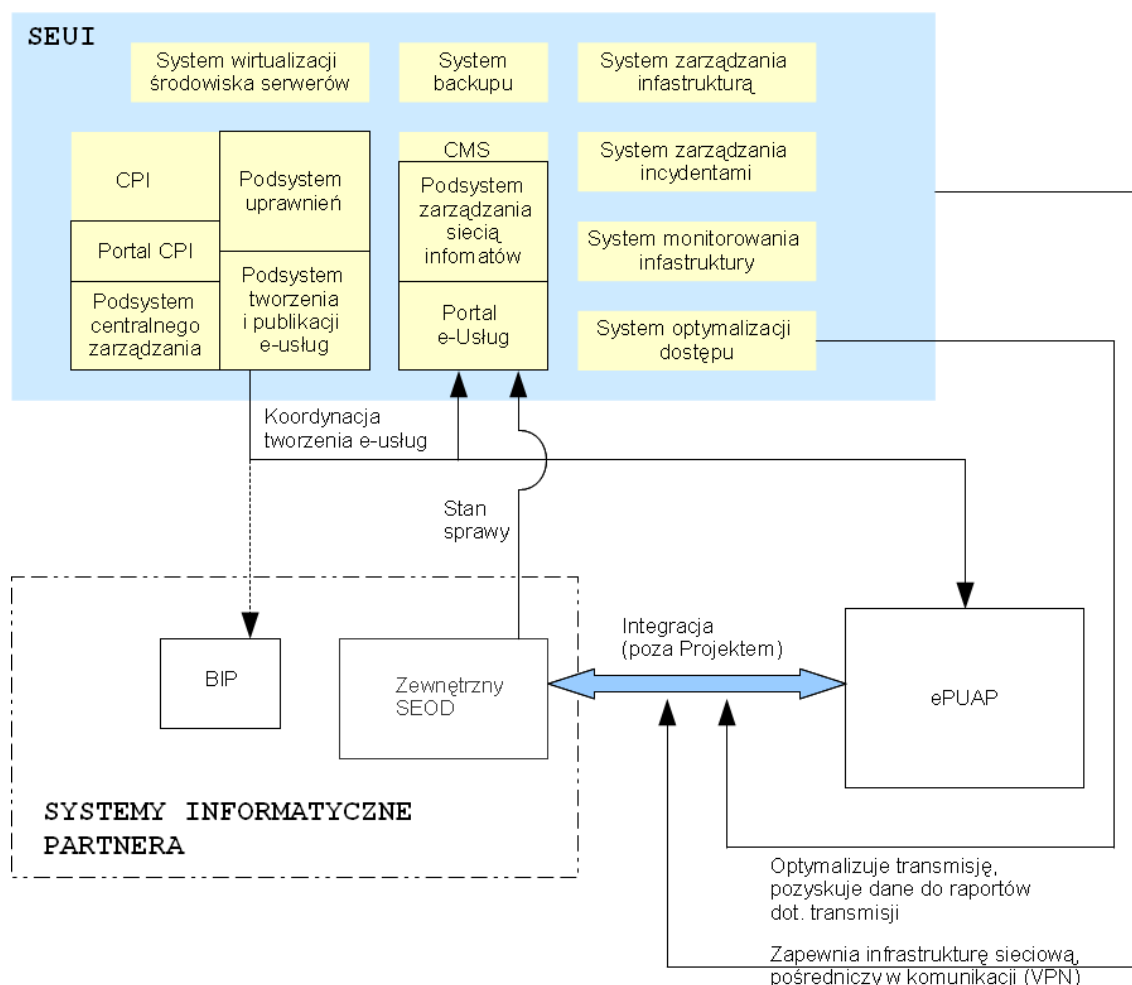
- obszar zaznaczony kolorem niebieskim oznacza SeUI,
- żółte prostokąty w ramach tego obszaru oznaczają poszczególne systemy składowe,
- w ramach żółtych prostokątów cienką ciągłą linią czarną wydzielone są poszczególne podsystemy,
- linia przerywana kreska-kropka wydziela obszar systemów Partnera, w ramach tych systemów kolorem jasno niebieskim oznaczone są systemy dostarczane w ramach Projektu,
- cienkie strzałki ciągłe oznaczają nadrzędność systemu/podsystemu, kierunek strzałki oznacza źródło informacji (skąd jest pobierana dokąd),
- strzałka z linią przerywaną (do BIP) oznacza powiązanie, które będzie opcjonalne, tzn. integracja może zostać zrealizowana przez Partnerów poza Projektem (w ramach Projektu powstanie interfejs od strony SEOD, do którego będzie można podpiąć dowolny system BIP),

- grube strzałki dwustronne wskazują na integrację (wymianę danych), opis określa czy jest ona realizowana w ramach Projektu czy poza nim.



**Rysunek 1: Architektura oprogramowania SeUI i SEOD**

Architekturę rozwiązania dla Partnerów, posiadających inny system elektronicznego obiegu dokumentów, nie dostarczany w ramach Projektu (nazwany „zewnętrznym SEOD”), przedstawia Rysunek 2.



**Rysunek 2: Architektura systemu SeUI zintegrowanego z zewnętrznym systemem elektronicznego obiegu dokumentów u Partnera**

Wykonawca w ramach zamówienia opracuje uszczegółowioną Architekturę Systemu PSeAP. W ramach tego dokumentu uwzględni oferowane komponenty gotowe oprogramowania oraz komponenty stworzone specjalnie na potrzeby Systemu PSeAP. Architektura systemu opracowana przez Wykonawcę powinna opisywać sposób współpracy i komunikacji tych komponentów, ich rozmieszczenie na dostarczonym sprzęcie oraz wskazywać w szczególności sposób realizacji i powiązania podsystemu uprawnień, podsystemu centralnego zarządzania oraz podsystemu tworzenia i publikacji e-usług.

---

## **7 Usługi publiczne systemu**

### **7.1 Usługi przewidziane do wdrożenia w ramach projektu PSeAP**

Ze względu na potrzeby niniejszego OPZ przyjęto następujące dwie klasyfikacje.

Pierwsza to podział usług ze względu na adresata, będą to więc:

- I) Usługi publiczne dla obywateli.
- II) Usługi publiczne dla organizacji społecznych i biznesowych.

Drugi podział usług związany jest z poziomem realizacji procesu którego usługa dotyczy, będą to więc następujące poziomy:

- I) Poziom 1. – informacyjny oznacza dostępność on-line (bezpośrednio w czasie rzeczywistym) informacji niezbędnej do rozpoczęcia jakiegoś procesu.
- II) Poziom 2. – jednokierunkowy, oznacza możliwość pobierania formularzy z oficjalnej strony podmiotu publicznego, aby po wydrukowaniu móc rozpocząć proces związany z daną usługą.
- III) Poziom 3. – dwukierunkowy, oznacza możliwość wypełnienia formularza na oficjalnej stronie podmiotu publicznego, niezbędny jest wtedy system autoryzacji osoby.
- IV) Poziom 4. – w pełni elektroniczny transakcyjny system, udostępniający usługi w całości poprzez sieć, włączając podejmowanie decyzji oraz dostarczanie jej. Nie jest potrzebna forma papierowa na żadnym etapie realizacji usługi.

Podstawowym punktem dostępowym do e-usług publicznych będzie Portal e-Usług wdrożony w ramach projektu PSeAP. Portal e-Usług będzie udostępniał katalog usług, formularze w formacie pdf do ściągnięcia oraz wsparcie i pomoc w zakresie elektronicznego załatwiania spraw. Jeśli obywatel będzie zainteresowany usługami na poziomie 3 lub 4, zostanie przekierowany do Portalu ePUAP, bezpośrednio na stronę danej usługi (lub ewentualnie innego systemu centralnego, realizującego usługę, np. CEIDG).

**Usługi na poziomie 1.** – oznaczają dostępność on-line informacji niezbędnej do rozpoczęcia jakiegoś procesu.

Lp.	Opis usługi
1.	Podatek rolny – osób fizycznych.
2.	Korekty gruntów rolnych – osoby fizyczne.
3.	Wygaśnięcia obowiązku podatku rolnego – osoby fizyczne.
4.	Podatek rolny – osoby prawne.
5.	Korekty gruntów rolnych – osoby prawne.
6.	Wygaśnięcia obowiązku podatku rolnego – osoby prawne.
7.	Podatek leśny – osoby fizyczne.
8.	Korekta podatku leśnego – osoby fizyczne.
9.	Wygaśnięcia obowiązku podatku leśnego – osoby fizyczne.
10.	Podatek leśny – osoby prawne.
11.	Korekta podatku leśnego – osoby prawne.
12.	Wygaśnięcia obowiązku podatku leśnego – osoby prawne.
13.	Podatek od nieruchomości – osoby fizyczne.
14.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby fizyczne.
15.	Korekta podatku od nieruchomości – osoby fizyczne.
16.	Dane nieruchomości – osoby fizyczne.

17.	Zwolnienia podatkowe w podatku od nieruchomości – osoby fizyczne.
18.	Wygaśnięcia obowiązku podatku od nieruchomości – osoby fizyczne.
19.	Podatek od nieruchomości – osoby prawne.
20.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby prawne.
21.	Korekta deklaracji na podatek od nieruchomości – osoby prawne.
22.	Dane nieruchomości – osoby prawne.
23.	Dane o zwolnieniach podatkowych w podatku od nieruchomości – osoby prawne.
24.	Wygaśnięcia obowiązku podatku od nieruchomości – osoby prawne.
25.	Podatek od środków transportowych – osoby fizyczne.
26.	Korekta podatku od środków transportowych – osoby fizyczne.
27.	Wygaśnięcia obowiązku podatkowego od środków transportowych – osoby fizyczne.
28.	Podatek od środków transportowych – osoby prawne.
29.	Korekty podatku od środków transportowych – osoby prawne.
30.	Wygaśnięcia obowiązku podatkowego od środków transportowych – osoby prawne.
31.	Wniosek o stwierdzenie nadpłaty podatku.
32.	Ulgi w podatkach (umorzenia, odroczenia, raty) – osoby fizyczne.
33.	Ulgi w podatkach (umorzenia, odroczenia, raty) – osoby prawne.
34.	Ulgi w podatkach od spadku i darowizn stanowiącym dochód gminy, a realizowanych przez urząd skarbowy.



35.	Ulgi w podatku od czynności cywilno-prawnych i karty podatkowej stanowiącym dochód gminy, a realizowanym przez urząd skarbowy.
36.	Zezwolenia na sprzedaż napojów alkoholowych.
37.	Zezwolenia na uprawę maku i konopi.
38.	Uzyskanie zezwoleń na zajęcie pasa drogowego pod lokalizację ogródków gastronomicznych.
39.	Zezwolenie na umieszczenie reklamy w pasie drogowym.
40.	Uzyskanie karty wędkarskiej i karty łowiectwa podwodnego.
41.	Rejestracja sprzętu pływającego służącego do połowu ryb.
42.	Zezwolenie na prowadzenie działalności w zakresie ochrony przed bezdomnymi zwierzętami.
43.	Zezwolenie na prowadzenie schronisk dla bezdomnych zwierząt.
44.	Zezwolenie na rozpowszechnianie i rozprowadzanie materiałów z zasobu geodezyjnego i kartograficznego.
45.	Dofinansowanie budowy i rozbudowy obiektów służących rehabilitacji ze środków PFRON.
46.	Dofinansowanie imprez sportowych i rekreacyjnych ze środków budżetu Gminy.
47.	Zmiany w miejscowym planie zagospodarowania przestrzennego.
48.	Zmiany decyzji o warunkach zabudowy lub lokalizacji inwestycji celu publicznego.
49.	Wydanie decyzji administracyjnej na prowadzenie robót w pasie drogi.
50.	Wydawanie zezwolenia na wykonywanie przewozów regularnych.
51.	Oznaczanie numerami porządkowymi nieruchomości.
52.	Wydawanie zaświadczenia o zgodności sposobu użytkowania obiektu budowlanego.

<b>53.</b>	Rozpatrywanie i zatwierdzanie projektów stałej organizacji ruchu.
<b>54.</b>	Uzgodnienie projektu budowlanego zjazdu, włączenia ulicy, budowy lub przebudowy drogi.
<b>55.</b>	Wydawanie warunków technicznych zasilania obcych odbiorników oświetleniowych z urządzeń oświetlenia ulicznego gminy.
<b>56.</b>	Wydawanie warunków technicznych dla budowy urządzeń oświetlenia ulicznego gminy.
<b>57.</b>	Nadanie imienia szkole lub placówce oświatowej.
<b>58.</b>	Zezwolenie na założenie szkoły lub placówki publicznej prowadzonej przez osobę prawną lub fizyczną.
<b>59.</b>	Wpis do ewidencji szkół niepublicznych.
<b>60.</b>	Uzyskanie środków finansowych na remont gminnej placówki oświatowej lub opiekuńczej (gimnazja, szkoły podstawowe, przedszkola).
<b>61.</b>	Dofinansowanie wypoczynku wyjazdowego/stacjonarnego zimowego i letniego dzieci i młodzieży organizowanego przez szkoły i oraz placówki oświatowe prowadzone przez gminę.
<b>62.</b>	Dofinansowanie krajowych wyjazdów śródrocznych uczniów szkół podstawowych lub gimnazjów prowadzonych przez gminę.
<b>63.</b>	Zasiłki szkolne.
<b>64.</b>	Dotacje na realizację zadań z dziedziny oświaty.
<b>65.</b>	Dotacje na zajęcia pozalekcyjne lub inne przedsięwzięcia dla szkół prowadzonych przez powiat.
<b>66.</b>	Stypendia socjalne ze środków unijnych dla uczniów szkoły ponadgimnazjalnej.
<b>67.</b>	Stypendia socjalne ze środków unijnych dla studentów z obszaru powiatu.
<b>68.</b>	Dofinansowanie obozów, seminariów i warsztatów naukowych uczniów szkół ponadgimnazjalnych prowadzonych przez gminę.
<b>69.</b>	Dotacje dla organizacji pozarządowych realizujących zadania z promocji i edukacji zdrowotnej.
<b>70.</b>	Dotacje na prowadzenie szkoły lub placówki oświatowej.

<b>71.</b>	Wywłaszczenie nieruchomości na rzecz Skarbu Państwa lub jednostek samorządu terytorialnego oraz ustalenie odszkodowania za wywłaszczenie nieruchomości.
<b>72.</b>	Ustalenie odszkodowania za nieruchomości przyjęte pod drogi gminne, powiatowe, wojewódzkie i krajowe.
<b>73.</b>	Zbywanie mieszkań będących własnością przedsiębiorstw państwowych.
<b>74.</b>	Wydanie karty parkingowej dla osób o obniżonej sprawności ruchowej.
<b>75.</b>	Przekształcenie prawa użytkowania wieczystego w prawo własności.
<b>76.</b>	Wydierżawienie gruntów stanowiących własność gminy.
<b>77.</b>	Opłaty z tytułu wieczystego użytkowania.
<b>78.</b>	Zwrot wywłaszczonej nieruchomości.
<b>79.</b>	Wykupienie mieszkania zakładowego.
<b>80.</b>	Wyłączenie gruntów z produkcji rolnej.
<b>81.</b>	Zmiana danych objętych ewidencją gruntów.
<b>82.</b>	Zajęcie nieruchomości.
<b>83.</b>	Odszkodowania za nieruchomości wydzielone pod drogi publiczne.
<b>84.</b>	Przyjęcie do zasobu operatu pomiarowego dotyczącego inwentaryzacji powykonawczej sieci oraz przyłączy uzbrojenia podziemnego.
<b>85.</b>	Przyjęcie do zasobu operatu pomiarowego dotyczącego podziału działki (przed wydaniem decyzji zatwierdzającej podział).
<b>86.</b>	Przyjęcie do zasobu operatu pomiarowego dotyczącego rozgraniczenia działki.
<b>87.</b>	Przyjęcie do zasobu operatu pomiarowego dotyczącego wznowienia znaków lub wyznaczenia punktów granicznych działek.
<b>88.</b>	Przyjęcie do zasobu operatu pomiarowego z inwentaryzacji powykonawczej budynku lub budowli.

89.	Wpis do ewidencji stowarzyszeń kultury fizycznej nieprowadzących działalności gospodarczej i ich związków.
90.	Wyciąg z ewidencji stowarzyszeń kultury fizycznej nieprowadzących działalności gospodarczej i ich związków .
91.	Wykreślenie z ewidencji stowarzyszeń kultury fizycznej nieprowadzących działalności gospodarczej i ich związków.
92.	Wpis do ewidencji klubów sportowych.
93.	Zawiadomienie o utracie dowodu osobistego..
94.	Wydanie wyciągu z ewidencji klubów sportowych.
95.	Wydanie wyciągu z ewidencji uczniowskich klubów sportowych.
96.	Wykreślenie z ewidencji klubów sportowych.
97.	Wykreślenie z ewidencji uczniowskich klubów sportowych.
98.	Zezwolenie na przeprowadzenie imprezy masowej.
99.	Zezwolenie na procesję, pielgrzymkę lub inne uroczystości o charakterze religijnym na drogach publicznych oraz drogach wewnętrznych gminy.
100.	Dotacja na organizację imprezy z zakresu kultury lub ochrony dóbr kultury albo sportu i turystyki.
101.	Nadanie uprawnień pilota wycieczek oraz przewodnika turystycznego.
102.	Wydawanie zezwoleń na wykorzystanie dróg w sposób szczególny.(imprezy na drogach)
103.	Utworzeniu stowarzyszenia zwykłego.
104.	<u>U</u> tworzenie terenowej jednostki organizacyjnej stowarzyszenia.
105.	Zmiana składu zarządu terenowej jednostki organizacyjnej stowarzyszenia, adresu jej siedziby oraz statutu stowarzyszenia.
106.	Pozwolenie na zbiórkę publiczną.

<b>107.</b>	Pożyczki z Funduszu Pracy na pokrycie kosztów szkolenia.
<b>108.</b>	Dofinansowanie kosztów studiów podyplomowych.
<b>109.</b>	Jednorazowe środki finansowe z Funduszu Pracy na działalność podejmowaną na zasadach określonych dla spółdzielni socjalnej.
<b>110.</b>	Refundacja kosztów opieki nad dzieckiem do lat 7 lub osobą zależną.
<b>111.</b>	Finansowanie kosztów egzaminu lub uzyskania licencji.
<b>112.</b>	Finansowanie szkolenia organizowanego przez PUP.
<b>113.</b>	Dotacja dla organizacji pozarządowych realizujących zadania z zakresu pomocy społecznej.
<b>114.</b>	Aktywizacja zawodowa repatrianta.
<b>115.</b>	Rozpatrywanie wniosków repatriantów o przyznanie pomocy na częściowe pokrycie kosztów związanych z remontem lub adaptacją lokalu mieszkalnego.
<b>116.</b>	Rozpatrywanie wniosków repatriantów o zwrot części kosztów poniesionych na podnoszenie kwalifikacji zawodowych.
<b>117.</b>	Rozpatrywanie wniosków pracodawców o zwrot części kosztów poniesionych na aktywizację zawodową zatrudnionego repatrianta.
<b>118.</b>	Pomoc dla repatriantów na podstawie decyzji Starosty.
<b>119.</b>	Nauczanie indywidualne.
<b>120.</b>	Kształcenie specjalne.
<b>121.</b>	Pobyty w ośrodkach wychowawczych.
<b>122.</b>	Wydawanie skierowania do kształcenia specjalnego (w specjalnych przedszkolach, szkołach i oddziałach specjalnych oraz ośrodkach).
<b>123.</b>	Dofinansowanie kosztów kształcenia pracodawcom, którzy zawarli z młodocianymi pracownikami umowę o pracę w celu przygotowania zawodowego.

<b>124.</b>	Uzyskanie orzeczenia o niepełnosprawności do 16 roku życia.
<b>125.</b>	Uzyskanie orzeczenia o stopniu niepełnosprawności.
<b>126.</b>	Uzyskanie orzeczenia o wskazaniach do ulg i uprawnień.
<b>127.</b>	Uzyskanie legitymacji osoby niepełnosprawnej.
<b>128.</b>	Uzyskanie karty parkingowej dla osoby niepełnosprawnej.
<b>129.</b>	Pożyczki ze środków PFRON.
<b>130.</b>	Przyznanie dofinansowania do likwidacji barier komunikacyjnych.
<b>131.</b>	Przyznanie dotacji do likwidacji barier architektonicznych.
<b>132.</b>	Dofinansowanie do turnusów rehabilitacyjnych dla osób niepełnosprawnych.
<b>133.</b>	Dofinansowanie do warsztatów terapii zajęciowych.
<b>134.</b>	Przystosowanie stanowiska pracy dla osoby niepełnosprawnej, adaptacja pomieszczeń i urządzeń do potrzeb osób niepełnosprawnych oraz kosztów zatrudnienia pracownika pomagającego pracownikowi niepełnosprawnemu.
<b>135.</b>	Zwrot kosztów wynagrodzeń i składek na ubezpieczenie społeczne dla pracodawców zatrudniających osoby niepełnosprawne.
<b>136.</b>	Pozwolenia na budowę obiektu budowlanego lub wykonania robót budowlanych.
<b>137.</b>	Uzyskanie oSTEMplowanego dziennika budowy.
<b>138.</b>	Zatwierdzenie projektu budowlanego.
<b>139.</b>	Pozwolenie na rozbiórkę obiektu budowlanego.
<b>140.</b>	Zgłoszenie obiektu budowlanego do rozbiórki.
<b>141.</b>	Wykonywanie obiektów budowlanych lub robót budowlanych niewymagających pozwolenia na budowę.

142.	Wydawanie zaświadczenia na przeprowadzenie badań psychologicznych.
143.	Zgłoszenie zmiany sposobu użytkowania obiektu budowlanego.
144.	Odstępstwo od warunków technicznych.
145.	Uzgadnianie dokumentacji projektowej.
146.	Wydanie wyrysu z operatu ewidencyjnego.
147.	Wydanie wypisu z operatu ewidencji gruntów i budynków.
148.	Wydanie zgody na budowę grobu murowanego.
149.	Wydanie zgody na rozłożenie na raty opłaty prolongacyjnej za nienaruszalność grobu ziemnego czasowego.
150.	Wydanie zgody na rozłożenie na raty opłaty prolongacyjnej za użytkowanie gruntu pod grób murowany.
151.	Wydanie zgody na remont grobu murowanego lub nagrobka.
152.	Wydanie zgody na wymianę lub montaż nagrobka.
153.	Wydanie zgody na dodatkowe zajęcie gruntu przy grobie murowanym lub ziemnym pod wylewkę rabatkę lub ławkę.
154.	Zaświadczenie o okresie pracy na gospodarstwie rolnym.
155.	Pozwolenie na krajowe przewozy drogowe na potrzeby własne osób lub rzeczy.
156.	Przyznanie uprawnień do prowadzenia badań technicznych pojazdów.
157.	Wpis do rejestru przedsiębiorców prowadzących stacje kontroli pojazdów.
158.	Wpis do rejestru przedsiębiorców prowadzących ośrodki szkolenia kierowców.
159.	Uzyskanie legitymacji instruktora nauki jazdy.

160.	Rozpatrywanie i i zatwierdzanie projektów stałej organizacji ruchu.
161.	Uzyskiwanie zezwolenia na czas określony i czas nieokreślony na przejazdy po drogach publicznych gminy pojazdów nie normatywnych.
162.	Pozwolenie wodno-prawne.
163.	Legalizacja urządzenia wodnego.
164.	Zatwierdzenie statutu spółki wodnej.
165.	Ustalenie wysokości i rodzaju świadczeń dla osób, które nie są członkami spółki wodnej, a odnoszą korzyści z urządzeń spółki lub przyczyniają się do zanieczyszczenia wody, dla której ochrony spółka powstała.
166.	Wydawanie decyzji ustalających linie brzegu dla wód śródlądowych nie będących wodami granicznymi oraz śródlądowymi drogami wodnymi.
167.	Wydawanie decyzji ustanawiających strefy ochronne ujęć wody obejmujące teren ochrony bezpośredniej.
168.	Pozwolenie na emisję pyłów i gazów do powietrza w związku z eksploatacją instalacji.
169.	Wyznaczenie miejsc postojowych dla osób niepełnosprawnych.
170.	Pozwolenie na wytwarzanie odpadów.
171.	Zatwierdzenie programu gospodarki odpadami niebezpiecznymi.
172.	Przyjmowanie informacja o wytwarzanych odpadach.
173.	Zezwolenie na prowadzenie działalności w zakresie zbierania i transportu odpadów.
174.	Wydawanie zaświadczenia o położeniu budynku.
175.	Udostępnienie informacji geologicznej.
176.	Zatwierdzenie projektu prac geologicznych.
177.	Wydanie koncesji na poszukiwanie i rozpoznawanie złóż kopalin.



<b>178.</b>	Wydanie koncesji na wydobywanie kopalin.
<b>179.</b>	Uzyskanie warunków rekultywacji powierzchni ziemi.
<b>180.</b>	Decyzje związane z rekultywacją gruntów zdewastowanych lub zdegradowanych w wyniku działalności przemysłowej.
<b>181.</b>	Zgłoszenie ofert pracy
<b>182.</b>	Pozwolenie na wycinkę drzew w lasach nie stanowiących własności Skarbu Państwa.
<b>183.</b>	Udostępnienie do wglądu dokumentacji budowlanej
<b>184.</b>	Wydanie decyzji na zmianę lasu na użytek rolny w przypadkach szczególnie uzasadnionych potrzeb właścicieli lasów.
<b>185.</b>	Wydawanie decyzji na pozyskanie drewna niezgodnie z uproszczonym planem urządzenia lasu w przypadku wypadków losowych.
<b>186.</b>	Wydawanie zezwolenia na odłów lub odstrzał redukcyjny zwierzyny, w przypadku szczególnego zagrożenia prawidłowego funkcjonowania obiektów produkcyjnych i użyteczności publicznej przez zwierzynę, oraz na odstąpienie od zakazu chwytania i przetrzymywania zwierzyny.
<b>187.</b>	Dotacja na pokrycie planowanych kosztów zalesienia gruntów.
<b>188.</b>	Dopuszczenie reproduktora do rozrodu naturalnego.
<b>189.</b>	Zezwolenie na posiadanie i hodowanie lub utrzymanie chartów rasowych lub ich mieszańców.
<b>190.</b>	Dopisanie współnajemcy.
<b>191.</b>	Zezwolenie na odłów lub odstrzał redukcyjny zwierzyny.
<b>192.</b>	Uznanie obiektu przyrodniczego za pomnik przyrody.
<b>193.</b>	Uznanie określonego terenu za użytek ekologiczny.
<b>194.</b>	Uznanie określonego terenu za zespół przyrodniczo-krajobrazowy.
<b>195.</b>	Założenie parku miejskiego.

---

<b>196.</b>	Utworzenie obszaru chronionego krajobrazu.
<b>197.</b>	Naliczanie kary pieniężnej za zniszczenie terenów zieleni albo drzew lub krzewów spowodowane niewłaściwym wykonywaniem robót ziemnych lub wykorzystywaniem sprzętu mechanicznego albo urządzeń technicznych oraz zastosowaniem środków chemicznych w sposób szkodliwy dla roślinności.
<b>198.</b>	Naliczenie kary pieniężnej za usuwanie drzew lub krzewów bez wymaganego zezwolenia.
<b>199.</b>	Nabijanie numerów na pojazdach
<b>200.</b>	Zgłoszenie budowy obiektów małej architektury w miejscach publicznych.

**Usługi na poziomie 2.** - oznaczają możliwość pobrania formularza, aby po wydrukowaniu móc rozpocząć proces związany z daną usługą.

Lp.	Opis usługi
1.	Zgłoszenie powstania obowiązku podatku rolnego – osoby fizyczne.
2.	Korekta informacji o gruntach rolnych – osoby fizyczne.
3.	Zgłoszenie wygaśnięcia obowiązku podatku rolnego – osoby fizyczne.
4.	Zgłoszenie powstania obowiązku podatku rolnego – osoby prawne.
5.	Korekta informacji o gruntach rolnych – osoby prawne.
6.	Zgłoszenie wygaśnięcia obowiązku podatku rolnego – osoby prawne.
7.	Zgłoszenie powstania obowiązku podatku leśnego – osoby fizyczne.
8.	Korekta deklaracji na podatek leśny – osoby fizyczne.
9.	Zgłoszenie wygaśnięcia obowiązku podatku leśnego – osoby fizyczne.
10.	Zgłoszenie powstania obowiązku podatku leśnego – osoby prawne.
11.	Korekta deklaracji na podatek leśny – osoby prawne.
12.	Zgłoszenie wygaśnięcia obowiązku podatku leśnego – osoby prawne.
13.	Zgłoszenie powstania obowiązku podatku od nieruchomości –osoby fizyczne.
14.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby fizyczne.
15.	Korekta deklaracji na podatek od nieruchomości – osoby fizyczne.
16.	Dane nieruchomości – osoby fizyczne.

---

17.	Dane o zwolnieniach podatkowych w podatku od nieruchomości – osoby fizyczne.
18.	Zgłoszenie wygaśnięcia obowiązku podatku od nieruchomości – osoby fizyczne.
19.	Zgłoszenie powstania obowiązku podatku od nieruchomości – osoby prawne.
20.	Korekta informacji o nieruchomościach obiektach budowlanych – osoby prawne.
21.	Korekta deklaracji na podatek od nieruchomości – osoby prawne.
22.	Dane nieruchomości – osoby prawne.
23.	Dane o zwolnieniach podatkowych w podatku od nieruchomości – osoby prawne.
24.	Zgłoszenie wygaśnięcia obowiązku podatku od nieruchomości – osoby prawne.
25.	Zgłoszenie powstania obowiązku podatku od środków transportowych –osoby fizyczne.
26.	Korekta deklaracji na podatek od środków transportowych – osoby fizyczne.
27.	Zgłoszenie wygaśnięcia obowiązku podatkowego od środków transportowych – osoby fizyczne.
28.	Zgłoszenie powstania obowiązku podatku od środków transportowych – osoby prawne.
29.	Korekta deklaracji na podatek od środków transportowych – osoby prawne.
30.	Zgłoszenie wygaśnięcia obowiązku podatkowego od środków transportowych – osoby prawne.
31.	Wniosek o stwierdzenie nadpłaty podatku.
32.	Wniosek o zaliczenie nadpłaty podatku na poczet przyszłych zobowiązań podatkowych.
33.	Wniosek o wydanie zezwolenia na sprzedaż napojów alkoholowych.
34.	Wniosek na wydanie zezwolenia na sprzedaż napojów alkoholowych dla przedsiębiorców, których działalność polega na organizacji przyjęć.

---

35.	Oświadczenie o wartości sprzedaży napojów alkoholowych.
36.	Wniosek o wydanie duplikatu zezwolenia na sprzedaż napojów alkoholowych.
37.	Wniosek na wydanie jednorazowego zezwolenia na sprzedaż napojów alkoholowych.
38.	Zezwolenie na uprawę maku i konopi.
39.	Wniosek o zmianę decyzji o warunkach zabudowy lub lokalizacji inwestycji celu publicznego.
40.	Zaświadczenie o przeznaczeniu terenów w miejscowych planach zagospodarowania przestrzennego
41.	Wniosek o oznaczenie numerami porządkowymi nieruchomości.
42.	Wniosek o wydanie zaświadczenia o zgodności sposobu użytkowania obiektu budowlanego.
43.	Wniosek o nadanie imienia szkole lub placówce oświatowej.
44.	Wniosek o wpis do ewidencji szkół niepublicznych.
45.	Wniosek o uzyskanie środków finansowych na remont gminnej placówki oświatowej lub opiekuńczej (gimnazja, szkoły podstawowe, przedszkola).
46.	Wniosek o dofinansowanie wypoczynku wyjazdowego/stacjonarnego zimowego i letniego dzieci i młodzieży organizowanego przez szkoły i oraz placówki oświatowe prowadzone przez gminę.
47.	Wniosek o dofinansowanie krajowych wyjazdów śródrocznych uczniów szkół podstawowych lub gimnazjów prowadzonych przez gminę.
48.	Wniosek o zasiłek szkolny.
49.	Wniosek o dotację na realizację zadań z dziedziny oświaty.
50.	Wniosek o dotację na zajęcia pozalekcyjne lub inne przedsięwzięcia dla szkół prowadzonych przez powiat.
51.	Wniosek o stypendium socjalne ze środków unijnych dla uczniów szkoły ponadgimnazjalnej.
52.	Wniosek o stypendium socjalne ze środków unijnych dla studentów z obszaru powiatu.

---

53.	Wniosek o dofinansowanie obozów, seminariów i warsztatów naukowych uczniów szkół ponad gimnazjalnych prowadzonych przez gminę.
54.	Wniosek o dotację dla organizacji pozarządowych realizujących zadania z promocji i edukacji zdrowotnej.
55.	Wniosek o dotację na prowadzenie szkoły lub placówki oświatowej.
56.	Wydanie karty parkingowej dla osób o obniżonej sprawności ruchowej.
57.	Wniosek o przekształcenie prawa użytkowania wieczystego w prawo własności.
58.	Wniosek o wydierżawienie gruntów stanowiących własność gminy.
59.	Wniosek o naliczenie lub aktualizację opłaty z tytułu wieczystego użytkowania.
60.	Wniosek o zwrot wywłaszczonej nieruchomości.
61.	Wniosek o wykupienie mieszkania zakładowego.
62.	Wniosek o przyznanie dodatku mieszkaniowego.
63.	Wniosek o wyłączenie gruntów z produkcji rolnej.
64.	Zgłoszenie zmian danych objętych ewidencją gruntów.
65.	Zezwolenie na zajęcie nieruchomości.
66.	Wniosek o udzielenie odszkodowania za nieruchomości wydzielone pod drogi publiczne.
67.	Wniosek o przyjęcie do zasobu operatu pomiarowego dotyczącego inwentaryzacji powykonawczej sieci oraz przyłączy uzbrojenia podziemnego.
68.	Wniosek o przyjęcie do zasobu operatu pomiarowego dotyczącego podziału działki (przed wydaniem decyzji zatwierdzającej podział).
69.	Wniosek o przyjęcie do zasobu operatu pomiarowego dotyczącego rozgraniczenia działki.
70.	Wniosek o przyjęcie do zasobu operatu pomiarowego dotyczącego wznowienia znaków lub wyznaczenia punktów granicznych działek.

---

<b>71.</b>	Wniosek o przyjęcie do zasobu operatu pomiarowego z inwentaryzacji powykonawczej budynku lub budowli.
<b>72.</b>	Wniosek o wpis do ewidencji stowarzyszeń kultury fizycznej nieprowadzących działalności gospodarczej i ich związków.
<b>73.</b>	Wniosek o wydanie wyciągu z ewidencji stowarzyszeń kultury fizycznej nieprowadzących działalności gospodarczej i ich związków.
<b>74.</b>	Wniosek o wykreślenie z ewidencji stowarzyszeń kultury fizycznej nieprowadzących działalności gospodarczej i ich związków.
<b>75.</b>	Wniosek o wpis do ewidencji klubów sportowych.
<b>76.</b>	Zawiadomienie o utracie dowodu osobistego.
<b>77.</b>	Wniosek o wydanie wyciągu z ewidencji klubów sportowych.
<b>78.</b>	Wniosek o wydanie wyciągu z ewidencji uczniowskich klubów sportowych.
<b>79.</b>	Wniosek o wykreślenie z ewidencji klubów sportowych.
<b>80.</b>	Wniosek o wykreślenie z ewidencji uczniowskich klubów sportowych.
<b>81.</b>	Zezwolenie na przeprowadzenie imprezy masowej.
<b>82.</b>	Wniosek o zgodę na procesję, pielgrzymkę lub inne uroczystości o charakterze religijnym na drogach publicznych oraz drogach wewnętrznych gminy.
<b>83.</b>	Wniosek o dotację na organizację imprezy z zakresu kultury lub ochrony dóbr kultury albo sportu i turystyki.
<b>84.</b>	Zawiadomienie o utworzeniu stowarzyszenia zwykłego.
<b>85.</b>	Zawiadomienie o utworzeniu terenowej jednostki organizacyjnej stowarzyszenia.
<b>86.</b>	Zawiadomienie o zmianie składu zarządu terenowej jednostki organizacyjnej stowarzyszenia, adresu jej siedziby oraz statutu stowarzyszenia.
<b>87.</b>	Wniosek o pozwolenie na zbiórkę publiczną.
<b>88.</b>	Wniosek o pożyczkę z Funduszu Pracy na pokrycie kosztów szkolenia.

89.	Wniosek o dofinansowanie kosztów studiów podyplomowych.
90.	Wniosek o jednorazowe środki finansowe z Funduszu Pracy na działalność podejmowaną na zasadach określonych dla spółdzielni socjalnej.
91.	Wniosek o refundację kosztów opieki nad dzieckiem do lat 7 lub osobą zależną.
92.	Wniosek o sfinansowanie kosztów egzaminu lub uzyskania licencji.
93.	Wniosek o dotację dla organizacji pozarządowych realizujących zadania z zakresu pomocy społecznej.
94.	Wniosek o orzeczenie niepełnosprawności do 16 roku życia.
95.	Wniosek o ustalenie terminu badania przez komisję ds. niepełnosprawnych.
96.	Wniosek o uzyskanie prawa do ulg i uprawnień.
97.	Wniosek o wydanie legitymacji osoby niepełnosprawnej.
98.	Wniosek o wydanie karty parkingowej dla osoby niepełnosprawnej.
99.	Wniosek o pożyczkę ze środków PFRON.
100.	Wniosek o dofinansowanie do likwidacji barier komunikacyjnych.
101.	Wniosek o dotację do likwidacji barier architektonicznych.
102.	Wniosek o dofinansowanie do turnusów rehabilitacyjnych dla osób niepełnosprawnych.
103.	Wniosek o dofinansowanie do warsztatów terapii zajęciowych.
104.	Wniosek o zwrot kosztów w związku z przystosowaniem stanowiska pracy dla osoby niepełnosprawnej, adaptacji pomieszczeń i urządzeń do potrzeb osób niepełnosprawnych oraz kosztów zatrudnienia pracownika pomagającego pracownikowi niepełnosprawnemu.
105.	Wniosek o zwrot kosztów wynagrodzeń i składek na ubezpieczenie społeczne dla pracodawców zatrudniających osoby niepełnosprawne.
106.	Wniosek o pozwolenie/przeniesienie pozwolenia na budowę obiektu budowlanego lub wykonania robót budowlanych.



107.	Wniosek o zatwierdzenie projektu budowlanego.
108.	Wniosek o pozwolenie na rozbiórkę obiektu budowlanego.
109.	Zgłoszenie obiektu budowlanego do rozbiórki.
110.	Zgłoszenie zamiaru wykonania obiektów budowlanych lub robót budowlanych niewymagających pozwolenia na budowę.
111.	Zgłoszenie zmiany sposobu użytkowania obiektu budowlanego.
112.	Wniosek o wyrys z operatu ewidencyjnego.
113.	Wniosek o wypis z operatu ewidencji gruntów i budynków.
114.	Wniosek o zgodę na budowę grobu murowanego.
115.	Wniosek o zgodę na rozłożenie na raty opłaty prolongacyjnej za nienaruszalność grobu ziemnego czasowego.
116.	Wniosek o zgodę na rozłożenie na raty opłaty prolongacyjnej za użytkowanie gruntu pod grób murowany.
117.	Zaświadczenie o opłacaniu składek na ubezpieczenie społeczne rolników.
118.	Wniosek o zgodę na wymianę lub montaż nagrobka.
119.	Wniosek o dodatkowe zajęcie gruntu przy grobie murowanym lub ziemnym pod wylewkę rabatki lub ławkę.
120.	Wniosek o uzyskanie licencji na wykonywanie krajowego transportu drogowego osób lub rzeczy.
121.	Wniosek o uzyskanie dodatkowego wypisu z licencji na krajowy transport drogowy osób lub rzeczy.
122.	Wniosek o pozwolenie na krajowe przewozy drogowe na potrzeby własne osób lub rzeczy.
123.	Wniosek o przyznanie uprawnień do prowadzenia badań technicznych pojazdów.
124.	Wniosek o wpis do rejestru przedsiębiorców prowadzących stacje kontroli pojazdów.

125.	Wniosek o pozwolenie wodno-prawne.
126.	Wniosek o legalizację urządzenia wodnego.
127.	Wniosek o zatwierdzenie statutu spółki wodnej.
128.	Wniosek o ustalenie wysokości i rodzaju świadczeń dla osób, które nie są członkami spółki wodnej, a odnoszą korzyści z urządzeń spółki lub przyczyniają się do zanieczyszczenia wody, dla której ochrony spółka powstała.
129.	Wniosek o pozwolenie na emisję pyłów i gazów do powietrza w związku z eksploatacją instalacji.
130.	Wyznaczenie miejsc postojowych dla osób niepełnosprawnych.
131.	Wniosek o pozwolenie na wytwarzanie odpadów.
132.	Wniosek o zatwierdzenie programu gospodarki odpadami niebezpiecznymi.
133.	Informacja o wytwarzanych odpadach.
134.	Wniosek o zezwolenie na prowadzenie działalności w zakresie zbierania i transportu odpadów.
135.	Wniosek o udostępnienie informacji geologicznej.
136.	Wniosek o zatwierdzenie projektu prac geologicznych.
137.	Wniosek na wydanie koncesji na poszukiwanie i rozpoznawanie złóż kopalin.
138.	Wniosek o wydanie koncesji na wydobywanie kopalin.
139.	Wniosek o uzyskanie warunków rekultywacji powierzchni ziemi.
140.	Zgłoszenie ofert pracy.
141.	Wniosek o dotację na pokrycie planowanych kosztów zalesienia gruntów.
142.	Wniosek o dopuszczenie reproduktora do rozrodu naturalnego.

143.	Wniosek o zezwolenie na posiadanie i hodowanie lub utrzymanie chartów rasowych lub ich mieszańców.
144.	Wniosek o zmianę lasu na użytek rolny w przypadkach szczególnie uzasadnionych potrzeb właścicieli lasów.
145.	Wniosek o zezwolenie na odłów lub odstrzał redukcyjny zwierzyny.
146.	Wniosek o uznanie obiektu przyrodniczego za pomnik przyrody.
147.	Wniosek o uznanie określonego terenu za użytek ekologiczny.
148.	Wniosek o uznanie określonego terenu za zespół przyrodniczo-krajobrazowy.
149.	Wniosek o założenie parku miejskiego.
150.	Wniosek o utworzenie obszaru chronionego krajobrazu.

**Usługi na poziomie 3.** – oznaczają możliwość wypełnienia formularza i wysłania go tego urzędu, niezbędny jest wtedy system autentyfikacji osoby, konieczna jest wizyta w urzędzie celem zakończenia procesu związanego z daną usługą.

Lp.	Opis usługi
1.	Zgłoszenie powstania obowiązku podatku rolnego – osoby fizyczne.
2.	Korekta informacji o gruntach rolnych – osoby fizyczne.
3.	Zgłoszenie wygaśnięcia obowiązku podatku rolnego – osoby fizyczne.
4.	Zgłoszenie powstania obowiązku podatku rolnego – osoby prawne.
5.	Korekta informacji o gruntach rolnych – osoby prawne.
6.	Zgłoszenie wygaśnięcia obowiązku podatku rolnego – osoby prawne.
7.	Zgłoszenie powstania obowiązku podatku leśnego – osoby fizyczne.

---

8.	Korekta deklaracji na podatek leśny – osoby fizyczne.
9.	Zgłoszenie wygaśnięcia obowiązku podatku leśnego – osoby fizyczne.
10.	Zgłoszenie powstania obowiązku podatku leśnego – osoby prawne.
11.	Korekta deklaracji na podatek leśny – osoby prawne.
12.	Zgłoszenie wygaśnięcia obowiązku podatku leśnego – osoby prawne.
13.	Zgłoszenie powstania obowiązku podatku od nieruchomości – osoby fizyczne.
14.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby fizyczne.
15.	Korekta deklaracji na podatek od nieruchomości – osoby fizyczne.
16.	Dane nieruchomości – osoby fizyczne.
17.	Dane o zwolnieniach podatkowych w podatku od nieruchomości – osoby fizyczne.
18.	Zgłoszenie wygaśnięcia obowiązku podatku od nieruchomości – osoby fizyczne.
19.	Zgłoszenie powstania obowiązku podatku od nieruchomości – osoby prawne.
20.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby prawne.
21.	Korekta deklaracji na podatek od nieruchomości – osoby prawne.
22.	Dane nieruchomości – osoby prawne.
23.	Dane o zwolnieniach podatkowych w podatku od nieruchomości – osoby prawne.
24.	Zgłoszenie wygaśnięcia obowiązku podatku od nieruchomości – osoby prawne.
25.	Zgłoszenie powstania obowiązku podatku od środków transportowych – osoby fizyczne.

---

26.	Korekta deklaracji na podatek od środków transportowych– osoby fizyczne.
27.	Zgłoszenie wygaśnięcia obowiązku podatkowego od środków transportowych – osoby fizyczne.
28.	Zgłoszenie powstania obowiązku podatku od środków transportowych – osoby prawne.
29.	Korekta deklaracji na podatek od środków transportowych - osoby prawne.
30.	Zgłoszenie wygaśnięcia obowiązku podatkowego od środków transportowych – osoby prawne.
31.	Wniosek o stwierdzenie nadpłaty podatku.
32.	Wniosek o zaliczenie nadpłaty podatku na poczet przyszłych zobowiązań podatkowych.
33.	Wniosek o wydanie zezwolenia na sprzedaż napojów alkoholowych.
34.	Wniosek na wydanie zezwolenia na sprzedaż napojów alkoholowych dla przedsiębiorców, których działalność polega na organizacji przyjęć.
35.	Oświadczenie o wartości sprzedaży napojów alkoholowych.
36.	Wniosek o wydanie duplikatu zezwolenia na sprzedaż napojów alkoholowych.
37.	Wniosek na wydanie jednorazowego zezwolenia na sprzedaż napojów alkoholowych.
38.	Wniosek o zezwolenie na uprawę maku i konopi.
39.	Wniosek o nadanie imienia szkole lub placówce oświatowej.
40.	Wniosek o wpis do ewidencji szkół niepublicznych.
41.	Wniosek o uzyskanie środków finansowych na remont gminnej placówki oświatowej lub opiekuńczej (gimnazja, szkoły podstawowe, przedszkola).
42.	Wniosek o dofinansowanie wypoczynku wyjazdowego/stacjonarnego zimowego i letniego dzieci i młodzieży organizowanego przez szkoły i oraz placówki oświatowe prowadzone przez gminę.
43.	Wniosek o dofinansowanie krajowych wyjazdów śródrocznych uczniów szkół podstawowych lub gimnazjów prowadzonych przez gminę.

44.	Wniosek o zasiłek szkolny.
45.	Wniosek o dotację na realizację zadań z dziedziny oświaty.
46.	Wniosek o dotację na zajęcia pozalekcyjne lub inne przedsięwzięcia dla szkół prowadzonych przez powiat.
47.	Wniosek o stypendium socjalne ze środków unijnych dla uczniów szkoły ponad gimnazjalnej.
48.	Wniosek o stypendium socjalne ze środków unijnych dla studentów z obszaru powiatu.
49.	Wniosek o dofinansowanie obozów, seminariów i warsztatów naukowych uczniów szkół ponad gimnazjalnych prowadzonych przez gminę.
50.	Wniosek o dotację dla organizacji pozarządowych realizujących zadania z promocji i edukacji zdrowotnej.

**Usługi poziomu 4.** – w pełni elektroniczny transakcyjny system, udostępniający usługi w całości poprzez sieć, włączając podejmowanie decyzji oraz dostarczanie jej. Nie jest potrzebna forma papierowa na żadnym etapie realizacji usługi.

Lp.	Opis usługi
1.	Zgłoszenie powstania obowiązku podatku rolnego – osoby fizyczne.
2.	Korekta informacji o gruntach rolnych – osoby fizyczne.
3.	Zgłoszenie wygaśnięcia obowiązku podatku rolnego – osoby fizyczne.
4.	Zgłoszenie powstania obowiązku podatku rolnego – osoby prawne.
5.	Korekta informacji o gruntach rolnych – osoby prawne.
6.	Zgłoszenie wygaśnięcia obowiązku podatku rolnego – osoby prawne.
7.	Zgłoszenie powstania obowiązku podatku leśnego – osoby fizyczne.
8.	Korekta deklaracji na podatek leśny – osoby fizyczne.

---

9.	Zgłoszenie wygaśnięcia obowiązku podatku leśnego – osoby fizyczne.
10.	Zgłoszenie powstania obowiązku podatku leśnego – osoby prawne.
11.	Korekta deklaracji na podatek leśny – osoby prawne.
12.	Zgłoszenie wygaśnięcia obowiązku podatku leśnego – osoby prawne.
13.	Zgłoszenie powstania obowiązku podatku od nieruchomości – osoby fizyczne.
14.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby fizyczne.
15.	Korekta deklaracji na podatek od nieruchomości – osoby fizyczne.
16.	Dane nieruchomości – osoby fizyczne.
17.	Dane o zwolnieniach podatkowych w podatku od nieruchomości – osoby fizyczne.
18.	Zgłoszenie wygaśnięcia obowiązku podatku od nieruchomości – osoby fizyczne.
19.	Zgłoszenie powstania obowiązku podatku od nieruchomości – osoby prawne.
20.	Korekta informacji o nieruchomościach i obiektach budowlanych – osoby prawne.

---

---

## 7.2 Wdrożenie e-usług

Wykonawca musi wdrożyć wszystkie 420 e-usług na poziomie 1 (informacja) dla wszystkich Partnerów Projektu świadczących usługi. Wdrożenie polegać będzie na wdrożeniu opisów i kart usług na Portalu e-Uслуг oraz wdrożeniu integracji z Katalogiem Usług Publicznych Platformy ePUAP (automatyczna aktualizacja). Karty usług zostaną sporządzone na podstawie danych od poszczególnych Partnerów. Opisy usług będą pochodziły z Platformy ePUAP, zaś w przypadku ich braku na ePUAP – zostaną opracowane przez Wykonawcę, skonsultowane z Partnerami z wykorzystaniem Portalu CPI i zatwierdzone przez Zamawiającego.

Dla każdej z e-usług wymaganych na poziomie 2, 3 i 4 Wykonawca zaprojektuje i wdroży po jednym standardowym formularzu oraz – dla e-usług poziomu 3 i 4 – w pełni skonfiguruje odpowiednie usługi na platformie ePUAP dla wszystkich podmiotów, które będą chciały korzystać z opracowanego standardowego formularza. Przez standardowe formularze rozumie się formularze o takim samym układzie i zawartości informacyjnej, różniące się tylko danymi podmiotu, do którego jest skierowany. Standardowe formularze będą uzgadniane przez Wykonawcę z zainteresowanymi podmiotami z wykorzystaniem Portalu CPI. Ponadto Wykonawca zobowiązany jest zaprojektować, skonsultować z Partnerami wskazanymi przez Zamawiającego i wdrożyć u nich dodatkowe formularze w liczbie 20 różnych formularzy (dla 20 lub więcej Partnerów, gdyż wolę korzystania z danego formularza może wyrazić wielu Partnerów). Na etapie analizy przedwdrożeniowej Zamawiający wskaże, których e-usług mają dotyczyć dodatkowe formularze.

Wdrożenie formularza u Partnera każdorazowo będzie polegało na zamieszczeniu go w ePUAP i skonfigurowaniu komunikacji z SEOD oraz udostępnieniu odpowiedniego formularza w SeUI do ściągnięcia, wydruku i wypełnienia ręcznie.

Wykonawca obowiązany jest wdrożyć sprawdzanie statusu spraw dla wszystkich spraw realizowanych w SEOD. Status spraw będzie mógł być sprawdzany przez klienta na Portalu e-Uслуг jedną z dwóch metod: na podstawie numeru wniosku i ewentualnych dodatkowych informacji sprawdzających (dla pojedynczych spraw) lub na podstawie identyfikacji klienta poprzez profil zaufany (dostęp do wszystkich spraw). Szczegóły, tzn. zakres informacji udzielanej klientowi w obu przypadkach i forma jej prezentacji, zostaną ustalone w trakcie analizy przedwdrożeniowej. Zakres ten powinien być konfigurowalny. SEOD w odpowiedzi na zapytanie z SeUI powinien zwracać plik XML, do którego w Portalu e-Uслуг przypisany jest plik XSL określający sposób prezentacji.



## 8 System e-usług internetowych

### 8.1 System zarządzania i monitoringu infrastruktury

#### 8.1.1 System zarządzania incydentami

	System zarządzania incydentami
SZI 1	System powinien współpracować z CPI w zakresie zgłaszania problemów technicznych oraz zapotrzebowania na zasoby IT (np. nowa maszyna wirtualna). Może to polegać na automatycznym przyjmowaniu i udostępnianiu statusów zgłoszeń przez CPI lub na tym, że rejestracja i monitorowanie zgłoszeń realizowane będą w całości i wyłącznie przez CPI.
SZI 2	System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
SZI 3	System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
SZI 4	System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
SZI 5	System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać: <ul style="list-style-type: none"> <li>A) optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,</li> <li>B) redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,</li> <li>C) automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,</li> <li>D) wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,</li> <li>E) planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,</li> <li>F) raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,</li> </ul>

	<p>G) tworzenie baz wiedzy na temat rozwiązywania problemów,</p> <p>H) automatyzację działań w przypadku znanych i opisanych problemów,</p> <p>I) wykrywanie odchyleń od założonych standardów ustalonych dla systemu.</p>
--	--

### 8.1.2 System wirtualizacji środowiska serwerów

	<b>System wirtualizacji środowiska serwerów</b>
SWŚS 1	System musi zapewnić możliwość optymalnego wykorzystania platform sprzętowych, dzięki możliwości zastosowania maszyn wirtualnych uruchamianych na maszynach fizycznych. Wymagane jest zapewnienie możliwości przenoszenia maszyn wirtualnych pomiędzy maszynami fizycznymi, nie powodując jednocześnie przerwy w pracy systemu hostów.
SWŚS 2	Maszyny wirtualne powinny mieć możliwość zarządzania zasobami sprzętowymi przydzielonymi do maszyn wirtualnych podczas normalnej pracy systemów. Środowisko powinno zapewnić mechanizmy niezawodnościowe pozwalające na odtworzenie maszyny podczas awarii.
SWŚS 3	Mechanizmy tworzenia maszyn wirtualnych powinny opierać się o funkcje wbudowane serwerowych systemów operacyjnych.
SWŚS 4	<p>Architektura Systemu zarządzania środowiskiem wirtualnym powinien składać się z:</p> <ul style="list-style-type: none"> <li>A) serwera zarządzającego,</li> <li>B) relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,</li> <li>C) konsoli, instalowanej na komputerach operatorów,</li> <li>D) portalu self-service (konsoli webowej) dla operatorów „departamentowych”,</li> <li>E) biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,</li> <li>F) agenta instalowanego na zarządzanych hostach wirtualizacyjnych,</li> <li>G) „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych,</li> <li>H) System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).</li> </ul>
SWŚS 5	<p><u>Interfejs użytkownika:</u></p> <ul style="list-style-type: none"> <li>A) Konsola musi umożliwiać wykonywanie codziennych zadań związanych</li> </ul>

	<p>z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.</p> <p>B) Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.</p> <p>C) Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres użycia procesora i podgląd na pulpit.</p> <p>D) Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.</p>
	<b>Scenariusze i zadania</b>
SWŚS 6	<p><u>Tworzenie maszyn wirtualnych</u></p> <p>A) System musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:</p> <ol style="list-style-type: none"> <li>Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny.</li> <li>Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych: <ul style="list-style-type: none"> <li>profilu sprzętowego,</li> <li>profilu systemu operacyjnego,</li> <li>przygotowanych dysków twardych.</li> </ul> </li> </ol> <p>B) Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.</p> <p>C) System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:</p> <ol style="list-style-type: none"> <li>w trybie migracji „on-line” – bez przerywania pracy,</li> <li>w trybie migracji „off-line” – z zapisem stanu maszyny.</li> </ol> <p>D) System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.</p> <p>E) System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.</p> <p>F) System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance” w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować</p>

	<p>migracją maszyn na inne hosty lub zapisaniem ich stanu.</p> <p>G) System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.</p>
--	--

### 8.1.3 System wirtualizacji środowiska serwerów- wymagania dodatkowe

	<b>System wirtualizacji środowiska serwerów – wymagania dodatkowe</b>
SWŚS 7	<p>A) System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna użycie współdzielonych zasobów przez jedną maszynę.</p> <p>B) System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczny bez potrzeby każdorazowego potwierdzenia.</p> <p>C) System musi kreować raporty z działania zarządzanego środowiska, w tym:</p> <ul style="list-style-type: none"> <li>i. użycie poszczególnych hostów,</li> <li>ii. trend w użyciu hostów,</li> <li>iii. użycie poszczególnych maszyn wirtualnych,</li> </ul> <p>D) System musi umożliwiać skorzystanie z szablonów:</p> <ul style="list-style-type: none"> <li>i wirtualnych maszyn,</li> <li>ii systemu operacyjnego gościa.</li> </ul> <p>E) System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).</p> <p>F) System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją).</p>

### 8.1.4 System tworzenia kopii zapasowych (backupu)

	<b>System backupu</b>
SB 1	System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać poniższe wymagania:
SB 2	<p>System musi składać się z:</p> <ul style="list-style-type: none"> <li>A) serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych,</li> <li>B) agentów kopii zapasowych instalowanych na komputerach zdalnych</li> <li>C) konsoli zarządzającej,</li> </ul>

	<p>D) relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,</p> <p>E) wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną.</p>
SB 3	System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service) lub równoważny. Wymaganie równoważności będzie uznane za spełnione, jeżeli system umożliwiać będzie automatyczne tworzenie kopii zapasowych i migawek danych, nawet jeśli mają one blokadę (lock) na określonym wolumenie, w określonym momencie w regularnych odstępach czasu. Ponadto system musi operować na poziomie bloków w systemie plikowym oraz gwarantować, że treść pliku nie będzie się zmieniała w trakcie robienia kopii zapasowej.
SB 4	System kopii zapasowych musi umożliwiać: <ul style="list-style-type: none"> <li>A) zapis danych na puli magazynowej złożonej z dysków twardych,</li> <li>B) zapis danych na bibliotekach taśmowych.</li> </ul>
SB 5	System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
SB 6	System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
SB 7	Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.
SB 8	System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
SB 9	System kopii zapasowych powinien umożliwiać przywrócenie: <ul style="list-style-type: none"> <li>A) danych plikowych,</li> <li>B) danych aplikacyjnych,</li> <li>C) stanu systemu (Systemstate),</li> <li>D) obrazu systemu operacyjnego (tzw. Bare Metal Restore).</li> </ul>
SB 10	System kopii zapasowych musi rozpoznawać aplikacje: <ul style="list-style-type: none"> <li>A) ze względu na tworzone logi transakcyjne:</li> </ul>

	<ul style="list-style-type: none"> <li>i Microsoft Exchange Server,</li> <li>ii Microsoft Office Sharepoint Server,</li> <li>iii Microsoft SQL Server.</li> </ul> <p>B) ze względu na zapewnienie nieprzerwalności pracy:</p> <ul style="list-style-type: none"> <li>i MicrosoftVirtual Server 2005,</li> <li>ii Microsoft Hyper-V server.</li> </ul>
SB 11	Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach.
SB 12	Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach.
SB 13	Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń.
SB 14	Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych.
SB 15	Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych.
SB 16	Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
SB 17	System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku.
SB 18	System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat.
SB 19	System kopii zapasowych musi umożliwiać odtworzenie danych do: <ul style="list-style-type: none"> <li>A) lokalizacji oryginalnej,</li> <li>B) lokalizacji alternatywnej,</li> <li>C) w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych.</li> </ul>

### 8.1.5 System optymalizacji dostępu

Celem systemu jest zapewnienie ciągłości dostępu do usług ePUAP oraz dostarczenie danych statystycznych związanych z jego wykorzystaniem. W tym celu lokalizacje JST muszą do usług ePUAP dostawać się za pośrednictwem SeUI, co znacznie poprawi przepustowość dostępu, zniweluje

---

opóźnienia oraz zapewni efektywne (zarówno kosztowo jak i funkcjonalnie) wykorzystanie systemów bezpieczeństwa.

System musi umożliwić akcelerację ruchu pomiędzy centralnym punktem styku WAN i lokalizacjami JST optymalizując dostęp do usług e-PUAP. Sieć WAN jest tu rozumiana jako sieć łącząca wszystkie JST z SeUI i SeUI z ePUAP. Nie będzie to jednak sieć wykorzystująca specjalne łącza do łączenia odległych komputerów lecz sieć wykorzystująca łącza do Internetu różnych dostawców z których korzystają JST. SeUI musi zapewnić techniki optymalizacji protokołów transportowych i aplikacyjnych, kompresję danych oraz inteligentne buforowanie. Wymagane są mechanizmy związane z zarządzaniem przesyłania danych wraz z przechowywaniem fragmentów transmisji w pamięci cache, co w przypadku transmisji danych zawierających znane już fragmenty pozwoli na przesłanie między urządzeniami jedynie wskaźników do tych fragmentów zapisanych w cache. System ma umożliwić osiągnięcie redukcji ilości danych przesyłanych przez łącza oraz poprawienie komfortu pracy z usługami ePUAP nawet w przypadku opóźnień i wysokiej stopy błędów na łączach zapewnionych przez operatorów.

W ramach postępowania wymagany jest dostarczenie do poszczególnych lokalizacji systemów realizujących opisaną powyżej funkcjonalność. Rozwiązanie powinno realizować mechanizmy optymalizacji co najmniej dla protokołów: http, CIFS, TCP.

Koniecznym jest również dostarczenie dla wszystkich mobilnych stacji – aplikacji pozwalającej na optymalizację ruchu z wykorzystaniem opisanych powyżej metod. Pakiety instalacyjne powinny być dostępne dla platformy środowiska pracy serwerów.

### **8.1.6 System operacyjny**

System operacyjny musi pełnić rolę platformy systemowej, na której będą uruchamiane poszczególne usługi. System musi także udostępniać katalog użytkowników służący do autentykacji użytkowników w ramach usług realizowanych przez projekt. Dodatkowo system operacyjny musi udostępnić dodatkowe, niezbędne usługi zapewniające spójność działania infrastruktury takie jak zarządzanie certyfikatami, usługami sieciowymi i inne. W zależności także od projektu architektury system operacyjny może być użyty jako platforma witalizacyjna dla pozostałych komponentów projektu takich jak bazy danych, serwery zarządzania treścią, aplikacja integrująca, serwery internetowe. Wymagania w zakresie systemów operacyjnych znajdują się w opisie oprogramowania standardowego.

### **8.1.7 Baza danych**

Bazy danych odpowiedzialne za przechowywanie informacji wytworzonych w poszczególnych komponentach rozwiązania. Wymagania w zakresie baz danych znajdują się w opisie oprogramowania standardowego.

## **8.2 Portal e-Uslug**

Wymaganie	Minimalne wymagania dotyczące dostawy i wdrożenia Portalu e-Uslug
-----------	---

	Ogólne
WPEU 1	<p>Portal e-Uслуг będzie systemem opartym o gotowe rozwiązanie do zarządzania treścią, wyspecyfikowane w rozdziale 10.8 – Serwer portalu internetowego. Wykonawca wdroży Portal e-Uслуг, który będzie złożony z następujących głównych elementów:</p> <ul style="list-style-type: none"> <li>A) część informacyjna (informacja o projekcie PSeAP, materiały promocyjne, instrukcje i informacje dotyczące korzystania z usług drogą elektroniczną, informacje o dostępnym wsparciu, informacje zamieszczane przez poszczególnych Partnerów Projektu „widoki informacyjne JST”);</li> <li>B) centrum pomocy dla klientów urzędów w zakresie korzystania z e-usług – dokumentacja, FAQ, wyszukiwanie w tematach pomocy, możliwość zgłaszania problemów i zadawania pytań;</li> <li>C) katalog usług – opisy i karty usług świadczonych przez poszczególnych Partnerów, formularze przeznaczone do wydruku i ręcznego wypełnienia przez klientów urzędów, bezpośrednio łączą do funkcjonalności składania wniosku na platformie ePUAP lub innych systemów centralnych (np. CEIDG, Empatia), wyszukiwarka usług;</li> <li>D) funkcjonalność sprawdzania statusu sprawy (lub po potwierdzeniu tożsamości z wykorzystaniem systemu identyfikacji i uwierzytelniania ePUAP), dla spraw załatwionych – przekierowanie do decyzji dostępnej elektronicznie na platformie ePUAP, ponadto dostęp do ewentualnych dodatkowych informacji generowanych dla klienta na żądanie z systemu SEOD (w przypadku wdrożenia odpowiednich interfejsów, np. dla podatków).</li> </ul>
WPEU 2	<p>W zakresie dostawy i wdrożenia Portalu e-Uслуг wymagane jest:</p> <ul style="list-style-type: none"> <li>A) Dostawa niezbędnych do uruchomienia Portalu e-Uслуг licencji: oprogramowania do zarządzania treścią (serwer portalu internetowego), motoru bazy danych oraz ewentualnego oprogramowania pomocniczego na potrzeby Portalu e-Uслуг, zgodnie z Architekturą Systemu opracowaną przez Wykonawcę, z uwzględnieniem dodatkowych licencji na potrzeby instancji szkoleniowej i instancji testowej systemu. Wymagania dotyczące dostarczanych licencji zawarto w rozdziale 16 niniejszego OPZ.</li> <li>B) Zaprojektowanie i wdrożenie Portalu e-Uслуг: <ul style="list-style-type: none"> <li>i. instalacja instancji produkcyjnej systemu na infrastrukturze wirtualnej w CPD, zapewnienie infrastruktury kopii zapasowych umożliwiającej codzienny backup zawartości Portalu e-Uслуг,</li> </ul> </li> </ul>



	<ul style="list-style-type: none"> <li>ii. konfiguracja systemu – inicjalizacja zmiennych i rejestrów systemowych, wprowadzenie do systemu danych administratorów i nadanie im odpowiednich uprawnień,</li> <li>iii. zaprojektowanie i wdrożenie struktury Portalu e-Uслуг, jego szaty graficznej, szablonów w zakresie prezentacji, menu,</li> <li>iv. zaprojektowanie, wdrożenie i konfiguracja procedur publikacyjnych w Portalu, w tym procedur tworzenia nowych opisów usług i kart usług z wykorzystaniem szablonów i formularzy oraz mechanizmu zatwierdzania i publikacji,</li> <li>v. zaprojektowanie i wykonanie integracji z ePUAP, oraz SEOD dostarczonym przez Wykonawcę,</li> <li>vi. zaprojektowanie i udostępnienie interfejsów integracyjnych do systemów BIP oraz systemów SEOD tych Partnerów, którzy nie wdrażają SEOD Wykonawcy.</li> <li>vii. wdrożenie Single Sign-On w obrębie całego systemu SeUI, zgodne technologicznie z ePUAP (SAML)</li> <li>viii. konfiguracja systemu w zakresie opracowania i wdrożenia wybranych treści oraz formularzy elektronicznych (zakres wyspecyfikowano poniżej),</li> <li>ix. wdrożenie opisów oraz kart usługi zestawu formularzy elektronicznych odpowiadających 420 usługom publicznym świadczonym przez JST Województwa Podkarpackiego,</li> <li>x. przeprowadzenie instruktażu stanowiskowego administratorów systemu,</li> <li>xi. przekazanie systemu do eksploatacji,</li> <li>xii. wdrożenie instancji szkoleniowej i testowej systemu na infrastrukturze wirtualnej u Lidera Projektu (będących kopią wdrożonej instancji produkcyjnej, zawierającej analogiczną konfigurację; instancja testowa powinna być zintegrowana</li> <li>xiii. z instancją testową ePUAP–jeśli będzie to możliwe od strony platformy ePUAP).</li> </ul>
WPEU 3	W zakresie katalogu usług Portal e-Uслуг musi umożliwiać wybór JST poprzez listę rozwijaną i poprzez mapę województwa z zaznaczonymi konturami JST.
WPEU 4	<p>Interfejs użytkownika musi być zgodny z wymaganiami dotyczącymi identyfikacji wizualnej Systemu, określonymi przez Zamawiającego w fazie Analizy Przedwdrożeniowej, a obejmującymi co najmniej:</p> <p>A) Klucz kolorystyczny interfejsu użytkownika.</p>

	B) Obrazy cyfrowe, symbole słowno - graficzne oraz inne informacje dotyczące Projektu, przeznaczone do umieszczenia w SeUI.
WPEU 5	Portal eUsług musi udostępniać co najmniej następujące metody wyszukiwania: A) przeszukiwanie pełnotekstowe i kontekstowe całości lub wybranych działów portalu, B) kontekstowe przeszukiwanie listy e-usług wg hierarchii słów kluczowych z mechanizmem podpowiedzi, C) przeszukiwanie wielokryterialne.
WPEU 6	Wyszukiwarka usług powinna umożliwiać administratorom przez wygodny interfejs dowolne grupowanie usług wg słów kluczowych w niezależne (alternatywne) drzewa hierarchii, które będą prezentowane klientom na Portalu (np. podatki – gruntowy, leśny, od psa; podatki – korekta, wniosek) oraz będą podstawą do mechanizmu wyszukiwania.  Ponadto automatycznie (na podstawie treści kart usług) usługi powinny być prezentowane w hierarchii urzędu – podziale na komórki urzędu, które się nimi w danym urzędzie zajmują. Lista komórek urzędu zaczerpnięta jest z konfiguracji SEOD lub może być wprowadzona ręcznie (dla urzędów z własnymi SEOD). Publikacja opisów i kart usług na Portalu e-Usług odbywa się z wykorzystaniem podsystemu tworzenia i publikacji e-usług.
WPEU 7	Katalog eUsług powinien umożliwiać alfabetyczne sortowanie usług lub sortowanie wg popularności.
WPEU 8	Katalog usług powinien prezentować co najmniej wszystkie informacje o każdej usłudze, które są przewidziane w Portalu ePUAP (opis, termin załatwienia, niezbędne dokumenty).
WPEU 9	Katalog usług musi umożliwiać rozpoczęcie od wyszukania usługi a potem wybór JST lub rozpoczęcie od wyboru JST celem dotarcia do właściwej usługi danego Partnera. Katalog usług musi umożliwiać łatwe i wygodne sprawdzenie z poziomu wyszukiwarki usług, czy do danej usługi jest w danej JST wdrożony formularz.
WPEU 10	System musi umożliwiać administratorom zamieszczanie formularzy pdf wygenerowanych automatycznie na podstawie e-formularzy XML zamieszczonych w CPI; zamieszczanie musi odbywać się poprzez Podsystem tworzenia i publikacji e-usług w CPI.
WPEU 11	Część informacyjna Portalu musi zawierać część wspólną oraz odrębny portal informacyjny dla każdego z obsługiwanych urzędów.

WPEU 12	<p>SeUI musi umożliwiać wprowadzanie informacji do portalu informacyjnego JST przynajmniej za pomocą wyszczególnionych poniżej mechanizmów:</p> <ul style="list-style-type: none"> <li>A) Bezpośrednia edycja treści portalu przez posiadających odpowiednie uprawnienia użytkowników.</li> <li>B) Automatyczny transfer dokumentów elektronicznych opublikowanych w SEOD odnośnej JST. W szczególności wdrożone zostanie przekazywanie na Portal aktów prawnych zatwierdzonych w SEOD.</li> </ul>
WPEU 13	<p>Zarządzanie treścią znajdującą się w portalu informacyjnym JST musi się odbywać za pomocą operacji na jednostce tematycznie powiązanych danych, określanej dalej jako „artykuł”. Artykuł może być tekstem (xml lub html), plikiem (treści multimedialne, pliki pdf do ściągnięcia itp.) lub grupą tych elementów. Każdy artykuł musi posiadać metadane (data publikacji, osoba publikująca, tytuł). Sposób prezentacji artykułów jest konfigurowalny niezależnie dla różnych części portalu, z możliwością dowolności lub wymuszenia określonego sposobu prezentacji przez uprawnionych administratorów.</p>
WPEU 14	<p>W odniesieniu do treści umieszczanej w portalu informacyjnym JST drogą bezpośredniej edycji, System musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Edycję menu portalu.</li> <li>B) Określanie reguł prezentacji dla danej gałęzi menu.</li> <li>C) Tworzenie nowych artykułów.</li> <li>D) Określanie terminu udostępnienia artykułu w portalu informacyjnym JST.</li> <li>E) Określanie terminu, po upływie którego artykuł przestanie być dostępny w portalu informacyjnym JST.</li> <li>F) Edytowanie tytułu artykułu.</li> <li>G) Edytowanie treści artykułu za pomocą edytora klasy WYSIWYG.</li> <li>H) Załączanie do artykułu plików zewnętrznych w dowolnym formacie.</li> </ul>
WPEU 15	<p>Portal e-Uслуг musi umożliwić narzucenie hierarchii menu i układu prezentacji artykułów dla poszczególnych JST oraz jednocześnie zezwolenie na dowolność publikacji w określonych gałęziach menu.</p> <p>Wykonawca musi wdrożyć menu i układ prezentacji oraz uprawnienia wg wymagań określonych w trakcie analizy przedwdrożeniowej.</p>
WPEU 16	<p>Portal e-Uслуг musi umożliwiać nadawanie uprawnień administratorom (tworzenie menu, tworzenie artykułów w gałęzi menu, modyfikacja menu, modyfikacja lub usuwanie artykułów i pozycji menu) w zakresie poszczególnych</p>

	gałęzi menu oraz poszczególnych JST.
WPEU 17	System musi umożliwiać skonfigurowanie procedury publikacji w Portalu e-Usług dla poszczególnych części portalu i poszczególnych JST tak, aby artykuł ukazywał się dopiero po zatwierdzeniu przez osobę upoważnioną.
WPEU 18	System musi umożliwiać modyfikację menu bez utraty artykułów i gałęzi podporządkowanych.
WPEU 19	Portal e-Usług musi spełniać warunki techniczne i organizacyjne przewidziane prawem dla Biuletynu Informacji Publicznej, w szczególności wskazane w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej w § 16-21.
WPEU 20	Portal e-Usług powinien umożliwiać radnym dostęp do: <ul style="list-style-type: none"> <li>A) projektów uchwał,</li> <li>B) protokołów z posiedzeń</li> <li>C) projektów budżetu,</li> <li>D) podjętych uchwał,</li> <li>E) danych statystycznych i analiz,</li> <li>F) oraz innych materiałów dystrybuowanych przez biuro rady.</li> </ul>

### 8.3 Centralny Portal Internetowy

Centralny Portal Internetowy	
Wymaganie	Wymagania ogólne
CPI 1	Centralny Portal Internetowy opisywać musi grupę funkcjonalności, umożliwiającą skoordynowane zarządzanie, rozwój i utrzymanie systemu PSeAP. Składać się on powinien z Portalu CPI, podsystemu uprawnień, podsystemu centralnego zarządzania oraz podsystemu tworzenia i publikacji e-usług.
CPI 2	Portal CPI oraz podsystem uprawnień powinien być portalem intranetowym o architekturze trójwarstwowej udostępnianym centralnie w oparciu o infrastrukturę sprzętową SeUI, natomiast nie wymaga się tego bezwzględnie w odniesieniu do pozostałych dwóch jego podsystemów.  Podsystemy centralnego zarządzania oraz tworzenia i publikacji e-usług zdefiniowane powinny być jako całości funkcjonalne, natomiast mogą być po części realizowane poprzez powiązane z CPI komponenty instalowane poza CPD, pod warunkiem zachowania interoperacyjności oraz pełnej integracji z CPI

	(w zakresie pracy grupowej, komentowania, wersjonowania i publikowania informacji, plików konfiguracyjnych, definicji usług, rekomendacji itp., a także ustawień np. w zakresie powiadomień).
	<b>Portal CPI – wymagania szczegółowe</b>
CPI 3	<p>A) Portal CPI musi pełnić dwie główne funkcje:</p> <ol style="list-style-type: none"> <li>zgłaszanie awarii i usterek,</li> <li>centrum pomocy i wsparcia dla administratorów w gminach,</li> </ol> <p>B) Portal musi być dostępny wyłącznie dla uprawnionych użytkowników Systemu PSeAP.</p> <p>C) Portal musi być oparty o dostarczone oprogramowanie serwera portalu internetowego.</p>
CPI 4	<p>W zakresie pomocy i wsparcia dla administratorów, portal CPI musi udostępniać:</p> <ol style="list-style-type: none"> <li>dokumentację systemów,</li> <li>pomoc dla użytkowników i administratorów systemu wraz z wyszukiwarką pełnotekstową oraz wg indeksu,</li> <li>mechanizm forum dyskusyjnego,</li> <li>FAQ i możliwość zadawania pytań przez formularz,</li> <li>narzędzia pracy grupowej wspierające pracę nad dokumentami i ich wersje robocze oraz ostateczne (aktualne i historyczne wraz z datami obowiązywania), komentowanie i ocenę dokumentów (dyskusja dot. dokumentu), mechanizm powiadamiania o nowych wersjach,</li> <li>komunikację między administratorami,</li> <li>kalendarze (wyświetlane oraz umożliwiające subskrypcję do SEOD).</li> </ol>
CPI 5	<p>W Portalu CPI muszą być opracowywane i konsultowane, przechowywane i udostępniane (wyświetlane):</p> <ol style="list-style-type: none"> <li>konfiguracje dot. usług, które będą co do zasady wdrażane jako jednolite, ale muszą być uzgodnione – opisy usług, formularze wniosków (system musi pozwalać na różnorodność, ale wykonawca wdraża konfigurację jednolitą domyślną),</li> <li>pliki konfiguracyjne, które mogą być przydatne dla wielu administratorów z różnych jednostek, w szczególności: wzory ścieżek obiegu, pliki konfiguracyjne dot. integracji z systemami dziedzinyowymi i BIP, szablony dokumentów.</li> </ol> <p>Mechanizmy te będą wykorzystywane przez Wykonawcę w trakcie wdrożenia.</p>
CPI 6	Portal CPI musi zawierać mechanizmy umożliwiające równoległą pracę wielu użytkowników nad dokumentami oraz możliwość oznaczenia w sposób

	widoczny dla innych, że ktoś w danym momencie pracuje nad dokumentem.
CPI 7	<p>Portal CPI musi:</p> <p>A) umożliwiać zgłaszanie oraz zarządzanie zgłoszeniami, związanymi z awariami elementów infrastruktury. Wyróżnia on rolę centralnych administratorów infrastruktury oraz lokalnych administratorów (przeznaczoną np. dla pracowników odpowiedzialnych za informatykę w poszczególnych urzędach).</p> <p>B) umożliwiać użytkownikowi śledzenie całego procesu związanego z obsługą zgłoszeń, począwszy od momentu rejestracji zgłoszenia, poprzez aktualizacje jego statusu, aż do momentu zamknięcia zgłoszenia.</p>
CPI 8	CPI powinien posiadać konfigurowalny formularz zgłoszenia awarii, umożliwiający m.in. jednoznaczną identyfikację: osoby zgłaszającej awarię, urządzenia lub komponentu systemu, którego zgłoszenie dotyczy, a także jego lokalizacji (na podstawie inwentarza infrastruktury prowadzonego w systemie zarządzania infrastrukturą); możliwe będzie załączanie plików do formularza zgłoszenia.
CPI 9	CPI musi umożliwiać dostęp do systemu uprawnionym użytkownikom SEOD(pełniących rolę administratorów centralnych lub lokalnych) bez konieczności podwójnego logowania; a także umożliwiać im odrębne zalogowanie się do systemu w przypadku awarii centralnego systemu autoryzacji.
CPI 10	CPI musi nadawać każdemu zgłoszeniu unikalny numer, umożliwiający jego szybkie wyszukanie.
CPI 11	Portal musi posiadać listę statusów zgłoszeń (w tym co najmniej: oczekujące, w naprawie, naprawione).
CPI 12	Portal musi umożliwiać przypisywanie zgłoszeniom etykiet z konfigurowalnego słownika (takich jak np. awaria krytyczna/usterka, awaria gwarancyjna/niegwarancyjna), przy czym możliwość taka powinna być dostępna zarówno dla zgłaszającego w ramach formularza (zakres zależny od konfiguracji formularza), jak i dla administratorów centralnych, obsługujących zgłoszenie (pełen zakres, możliwość zmiany wcześniej nadanych etykiet);

CPI 13	Portal musi umożliwiać zgłaszającemu sprawdzenie treści, statusu, etykiet i historii zgłoszenia oraz głównej osoby przypisanej do jego obsługi (imię, nazwisko, adres e-mail, telefon) na podstawie numeru zgłoszenia; to samo uprawnienie przysługuje wszystkim administratorom lokalnym w JST, której zgłoszenie dotyczy.
CPI 14	Portal musi umożliwiać na etapie wypełniania formularza zgłoszenia zastrzeżenie jego treści – wówczas dla innych uprawnionych do podglądu zgłoszenia administratorów lokalnych nie będzie dostępna treść zgłoszenia, lecz tylko pozostałe informacje – status, historia, osoba obsługująca, osoba zgłaszająca.
CPI 15	Portal musi umożliwiać administratorom lokalnym wyświetlanie, filtrowanie i sortowanie listy zgłoszeń (z wyróżnieniem i możliwością odfiltrowania zgłoszeń własnych, ze swojej jednostki, dot. urzędzeń, za które jest odpowiedzialny) wg złożonych kryteriów (jakiego urzędzenia lub grupy urzędzeń dotyczy, wg słów kluczowych, wg statusów, wg dat ostatniej zmiany statusu, wg etykiet); a także dostęp do szczegółów poszczególnych zgłoszeń z poziomu tej listy.
CPI 16	Portal musi umożliwiać poszczególnym administratorom lokalnym włączenie powiadomień (e-mail, sms) dot. zmiany statusu zgłoszenia – poprzez ustawienia domyślne oraz ewentualne nadpisanie tych ustawień dla konkretnego zgłoszenia.
CPI 17	Portal musi umożliwiać administratorom centralnym agregację i przetwarzanie w ramach jednej procedury kilku zgłoszeń, dotyczących tej samej awarii (zmiany statusu i automatyczne powiadomienia dotyczą wtedy wszystkich zgłoszeń tej awarii).
CPI 18	Portal musi umożliwiać administratorom centralnym zmianę statusu zgłoszenia.
CPI 19	Portal musi umożliwiać wyznaczenie osoby głównej odpowiedzialnej za zgłoszenie, co odbywa się musi automatycznie na podstawie formularza (w zależności od komponentu którego zgłoszenie dotyczy, przy czym system umożliwia konfigurację dodatkowych kryteriów).  Zgłoszenie musi być przypisywane przez system zdefiniowanej grupie administratorów, którzy „pobierają” zgłoszenia do realizacji. „Pobranie” zgłoszenia musi powodować automatyczną zmianę statusu i określenie osoby odpowiedzialnej za zgłoszenie.
CPI 20	Portal musi umożliwiać administratorom centralnym tworzenie i delegowanie do innych administratorów centralnych (lub ich grup) zadań cząstkowych do wykonania w ramach usuwania awarii wraz z terminami ich wykonania, co nie

	zmienia głównej osoby odpowiedzialnej za zgłoszenie;
CPI 21	Portal musi umożliwiać zmianę osób odpowiedzialnych za obsługę zgłoszenia i poszczególnych zadań;
CPI 22	Portal musi umożliwiać poszczególnym administratorom obsługującym zgłoszenie na dodawanie dowolnych notatek i zdarzeń, związanych z jego realizacją na każdym etapie;
CPI 23	Portal musi umożliwiać zgłaszanie gwarancyjnych awarii sprzętu i oprogramowania z poziomu systemu oraz monitorowanie terminowej realizacji napraw gwarancyjnych.
CPI 24	Portal musi umożliwiać monitorowanie czasu i terminowości usuwania awarii oraz realizacji zadań i zgłoszeń przez poszczególnych pracowników.
CPI 25	Portal musi umożliwiać generowanie statystyk i raportów (w formacie pdf, xls, doc., dot. różnych rodzajów awarii, pracowników, grup pracowników, urzędzeń; system powinien umożliwić konfigurację dowolnych raportów, przy czym wykonawca uzgodni z zamawiającym i wdroży następujące raporty: historia awarii i napraw zadanego urządzenia, awaryjność poszczególnych urzędzeń, średni czas naprawy i średnia liczba wystąpień różnego rodzaju awarii (wg etykiet awarii i klas urzędzeń) w zadanym przedziale czasu, liczba, średni czas i terminowość realizacji zadań przez pracownika lub grupę pracowników.
CPI 26	Portal musi wspierać priorytetyzację zadań administratorów centralnych z uwzględnieniem terminów skonfigurowanych dla różnego typu awarii i urzędzeń oraz terminów zadań częściowych.
CPI 27	Portal musi udostępniać administratorom centralnym listę zgłoszeń i zadań im przypisanych oraz listę zgłoszeń nowych (do „pobrania”), a także listę zgłoszeń historycznych, z możliwością filtrowania i sortowania poszczególnych list wg różnych kryteriów, w tym priorytetu, terminu załatwienia; terminu zgłoszenia i innych.
CPI 28	Portal musi przysyłać automatyczne powiadomienia e-mailem lub sms-em o zgłoszeniach awarii do administratorów centralnych, umożliwiać im konfigurację powiadomień w zależności od kategorii zgłoszenia (np. błąd krytyczny, usterka);
CPI 29	Portal musi umożliwiać dostęp do informacji o zadaniach pracowników podległych oraz narzędzia monitorowania pracy zespołu przez przełożonego.
	<b>Podsystem centralnego zarządzania</b>



CPI 30	Podsystem centralnego zarządzania ma za zadanie ułatwienie rozwiązywania problemów z oprogramowaniem systemu PSeAP instalowanym poza CPD PSeAP i jego konfiguracją.
CPI 31	Podsystem musi pozwalać na realizację zarządzania oprogramowaniem SEOD u Partnerów oraz jego integracją z ePUAP m.in. w zakresie aktualizacji oprogramowania oraz interfejsów integracyjnych oprogramowania (m.in. półautomatyczna aktualizacja, monitorowanie wersji i wybranych aspektów konfiguracji, powiadamianie o nowych wersjach i poprawkach).
CPI 32	Podsystem musi zapewnić dostęp do podstawowych informacji technicznych o systemach SEOD u Partnerów oraz zapewni możliwość bezpiecznego dystrybuowania aktualizacji kodu oraz konfiguracji interfejsów.  W przypadku istnienia komponentów SeUI instalowanych lokalnie na komputerach użytkownika, podsystem centralnego zarządzania musi umożliwić także wykrywanie wersji oraz udostępnianie automatycznych aktualizacji dla tych komponentów.
CPI 33	Podsystem musi prezentować administratorom informacje dot. zakresu i wersji poszczególnych komponentów oprogramowania, poprawek oraz konfiguracji zainstalowanych u Partnerów poprzez czytelne zestawienia z możliwością filtracji i sortowania wg dowolnych kolumn (m.in. Partner, komponent, wersja). Z poziomu tego interfejsu musi być możliwość zarządzania aktualizacją.
CPI 34	Podsystem centralnego zarządzania będzie użytkowany przez administratorów centralnych, mających dostęp do informacji o komponentach u wszystkich Partnerów, oraz lokalnych administratorów Partnerów, mających dostęp do informacji o komponentach u danego Partnera. Zakres możliwych czynności poszczególnych administratorów musi być regulowany przez system uprawnień.
CPI 35	<u>Zarządzanie aktualizacją</u> musi obejmować: <ul style="list-style-type: none"> <li>A) możliwość definiowania dla poszczególnych komponentów i Partnerów, czy aktualizacja ma być automatyczna, czy musi być każdorazowo zatwierdzana przez lokalnego administratora,</li> <li>B) możliwość dokonania przez centralnych administratorów automatycznej aktualizacji dla jednego lub wielu Partnerów lub powiadomienia lokalnych administratorów o dostępności nowszych wersji,</li> <li>C) możliwość wykonania aktualizacji poszczególnych komponentów przez lokalnych administratorów,</li> <li>D) możliwość wyboru instalowanych poprawek i konfiguracji, podglądu poprawek i konfiguracji nie zainstalowanych a dostępnych,</li> </ul>

	E) możliwość definiowania terminu aktualizacji z wyprzedzeniem, z dokładnością co najmniej do minuty.
CPI 36	Aktualizacja i dystrybucja wersji i konfiguracji oprogramowania musi się odbywać w sposób bezpieczny, tzn. pliki muszą być zabezpieczone podpisem cyfrowym zapewniającym integralność i niezaprzeczalność co do źródła, zaś sam proces aktualizacji musi być realizowany w taki sposób, by zapewnić pełne zabezpieczenie przed przypadkowym zniszczeniem lub nadpisaniem danych oraz zapewnić backup bezpośrednio przed aktualizacją.  Musi być dopuszczona możliwość aktualizacji SEOD w oknach serwisowych poza godzinami pracy urzędów i zatrzymanie systemu na czas aktualizacji.
CPI 37	Podsystem centralnego zarządzania musi zawierać repozytorium historycznych wersji i poprawek poszczególnych komponentów systemu oraz historię aktualizacji dla każdego Partnera.
CPI 38	Podsystem centralnego zarządzania musi uwzględniać instancje szkoleniowe i testowe oraz umożliwi odnotowywanie wersji testowych i odróżnianie ich od wersji stabilnych.
CPI 39	Podsystem centralnego zarządzania musi umożliwić dodawanie nowych wersji oprogramowania, poprawek („łatek”), nowych wersji konfiguracji.
CPI 40	Podsystem centralnego zarządzania musi być ściśle powiązany z Portalem CPI, który musi umożliwiać przygotowywanie i konsultowanie konfiguracji, które po opracowaniu, przetestowaniu i zatwierdzeniu będą dystrybuowane w podsystemie centralnego zarządzania. Ponadto Portal CPI musi służyć odnotowywaniu i rozwiązywaniu problemów, które będą związane z określonymi komponentami, wersjami, aktualizacjami i konfiguracjami.
CPI 41	Dopuszcza się realizację podsystemu centralnego zarządzania z wykorzystaniem komponentów instalowanych poza CPD, np. komponentów wchodzących w skład SEOD, zainstalowanych na serwerach SEOD u Partnerów.  Dopuszcza się także realizację dodatkowych funkcji administracyjnych oferowanych przez wykonawcę poza interfejsem przeglądarkowym.
	<b>Podsystem tworzenia i publikacji e-usług</b>
CPI 42	A) Podsystem musi umożliwiać poprzez graficzny interfejs tworzenie, modyfikację, publikację i konfigurację usług w Portalu eUsług i ePUAP, w tym – wzorów dokumentów elektronicznych, opisów („kart”) usług, formularzy elektronicznych. Podsystem musi być zintegrowany z systemami ePUAP oraz SEOD.

	<p>B) Podsystem musi być wyposażony w graficzny edytor formularzy elektronicznych oraz narzędzia wspierające poszczególne etapy tworzenia usługi z przeznaczeniem na portal ePUAP (karta usługi, formularz, konfiguracja skrytki, aplikacja ePUAP). Formularze muszą być tworzone w technologii XForms.</p>
CPI 43	<p>A) Podsystem musi umożliwiać automatyzację dodawania nowych usług i musi być w tym zakresie zintegrowany z ePUAP oraz musi wystawiać interfejs (do eksportu i importu kart i opisów usług oraz formularzy) dla zewnętrznych systemów BIP oraz komunikować się z SEOD (co najmniej: import struktury urzędu celem stworzenia opisów usług świadczonych przez poszczególne komórki).</p> <p>B) Dodanie/modyfikacja/usunięcie usługi musi być realizowane kompleksowo przez podsystem, tzn. dodanie/modyfikacja/usunięcie usługi spowoduje automatyczne pojawienie się odpowiednich elementów na Portalu eUsług (informacja, formularz do ściągnięcia, linki), w Portalu ePUAP (automatyczna aktualizacja katalogu usług publicznych oraz pozostałych elementów konfiguracji w zakresie możliwości stwarzanych przez platformę – wymagane jest co najmniej wygenerowanie plików konfiguracyjnych do ręcznego załadowania, jeśli nie będzie możliwe automatyczne dokonanie zmian), w SEOD (repozytorium formularzy wniosków, które mogą inicjować sprawę i które można wykorzystać w ścieżkach przetwarzania), jak również w zintegrowanych systemach BIP. Nadrzędnym systemem, skąd przekazywane są dane do innych, jest Portal e-Usług PSeAP. Wyjątkiem są opisy usług na Platformie ePUAP, które są źródłem dla Portalu.</p>
CPI 44	<p>Dla nowo tworzonych/modyfikowanych usług podsystem musi zapewnić możliwość stworzenia formularza w graficznym edytorze o funkcjonalności nie gorszej niż aplikacja dostępna na platformie ePUAP. Dopuszcza się dostawę gotowego rozwiązania licencjonowanego w tym zakresie (liczba licencji dla każdego Partnera ma być równa liczbie administratorów u tego Partnera, dodatkowo wymagana jest instancja testowa i szkoleniowa w CPD).</p> <p>Wygenerowany formularz powinien działać prawidłowo jako formularz e-usługi po załadowaniu na Platformę ePUAP.</p> <p>A) Aplikacja powinna komunikować się z repozytorium wzorów dokumentów i zapewniać, że schematy atomowe ePUAP(np. adres) będą dostępne jako pola - składowe formularzy, przy czym można umieścić takie pola w formularzu metodą przeciągnij-i-upuść</p> <p>B) Formularze tworzone z wykorzystaniem aplikacji powinny być zgodne ze schematami wykorzystywanymi na platformie ePUAP (w obrębie</p>

	<p>aplikacji wymaga się weryfikacji formularzy pod kątem zgodności z ePUAP oraz automatycznego wykorzystania obowiązujących na ePUAP schematów i elementów)</p> <p>C) Aplikacja powinna umożliwiać edycję w trybie kodu źródłowego oraz graficznym</p> <p>D) Aplikacja powinna umożliwiać import i eksport formularza oraz jego modyfikację.</p>
CPI 45	<p>Podsystem musi umożliwić tworzenie formularzy na potrzeby elektronicznego obiegu dokumentów, które mogą być elementem na ścieżce sprawy i mogą być automatycznie wypełniane wybranymi danymi, np. z nadesłanego wniosku (mapowanie pól). Dopuszcza się zastosowanie dwóch różnych edytorów dla e-formularzy SEOD i dla e-formularzy przeznaczonych dla klientów.</p>
CPI 46	<p>Podsystem musi zapewnić możliwość definiowania i przechowywania wzorów dokumentów, formularzy i usług w takiej postaci, aby można było je łatwo załadować na platformę ePUAP lub do systemu SEOD dla każdego z Partnerów. Definicje te powinny być wersjonowane oraz podlegać pracy grupowej (np. poprzez tworzenie kolejnych wersji roboczych zgodnie z uprawnieniami, zakończone publikacją w Portalu CPI wersji gotowej, która może być wykorzystana przez poszczególnych Partnerów).</p>
CPI 47	<p>Funkcjonalność związana z edytorem formularzy elektronicznych musi być realizowana przez lokalny komponent, który może być samodzielną aplikacją licencjonowaną przez podmioty trzecie. W tym przypadku wymaga się dostarczenia co najmniej liczby licencji odpowiadającej liczbie administratorów w poszczególnych podmiotach, wg tabeli zamieszczonej w załączniku nr 2 do OPZ.</p>
	<b>Podsystem uprawnień</b>
CPI 48	<p>A) Zarządzanie uprawnieniami administracyjnymi, dotyczącymi wszystkich elementów SeUI (Portal e-Uslug, CPI, systemy zarządzania i monitoringu infrastruktury), musi być scentralizowane dla wszystkich aplikacji składowych SeUI.</p> <p>B) Musi być dostępny jeden spójny interfejs (GUI), w którym zarządza się wszystkimi użytkownikami i ich uprawnieniami do aplikacji składowych SeUI.</p>
CPI 49	<p>Podsystem uprawnień musi umożliwić łączenie uprawnień w grupy (role) i nadawać je użytkownikom, wskazując dodatkowo podmiot, którego uprawnienia tego użytkownika będą dotyczyć.</p>

CPI 50	Scentralizowane zarządzanie uprawnieniami musi dotyczyć także ewentualnych komponentów SeUI zrealizowanych poprzez komponent lokalnie instalowany na komputerze użytkownika, jeżeli takie wystąpią.
CPI 51	Podsystem uprawnień musi umożliwiać nadawanie uprawnień do pracy w SeUI zarejestrowanym administratorom SEOD oraz innym (nowym) użytkownikom – np. partnerem posiadającym własne SEOD. System uprawnień musi umożliwiać przypisywanie uprawnień do stanowisk lub osób i umożliwi konfigurowalne monity do administratorów nadrzędnych w przypadku zmiany osób na danym stanowisku.
CPI 52	Podsystem uprawnień musi umożliwić nadawanie roli (grupy uprawnień) w kontekście konkretnego Partnera.
CPI 53	Podsystem uprawnień musi być skonfigurowany tak, by wyróżniał szczególną grupę administratorów centralnych
CPI 54	Podsystem uprawnień umożliwi delegowanie uprawnień i cofanie delegacji. Uprawnienie do delegacji uprawnień jest dodatkowym uprawnieniem.

#### 8.4 Wdrożenie e-usług

Wymaganie	Wdrożenie e-usług
WDEU 1	Do obowiązków wykonawcy w zakresie wdrożenia e-usług będzie należało wdrożenie e-usług wg listy zawartej w rozdziale 7.1 zarówno na Portalu e-Uслуг, jak i na platformie ePUAP zgodnie z zakresem opisanym w rozdziale 7.2 „Wdrożenia e-usług”. Wskazane poziomy odnoszą się do front office, czyli sposobu załatwienia sprawy z perspektywy klienta. W zakresie back office, tzn. od przyjęcia dokumentu do systemu obiegu dokumentów aż do nadania odpowiedzi za potwierdzeniem doręczenia, zakres wdrożenia przedstawiony jest w wymaganiach dotyczących wdrożenia SEOD.
WDEU 2	Wykonawca musi przeprowadzić analizę przedwdrożeniową w zakresie e-usług; w wyniku analizy muszą być przez wykonawcę opracowane opisy oraz karty usług w formie plików XML. Zawartość opisów oraz kart usług musi być zgodna z wymaganiami platformy ePUAP (muszą być wszystkie elementy treściowe, występujące w opisach i kartach usług), ponadto mogą w strukturze wystąpić informacje dodatkowe (np. numery kont do wpłat), jeśli wykaże taką potrzebę analiza przedwdrożeniowa.
WDEU 3	Wykonawca musi opracować transformaty XSLT, umożliwiające konwersję kart i opisów usług na pliki XML, które mogą być załadowany (automatycznie bądź

	manualnie) na platformę ePUAP oraz na pliki, które będą prezentowane w SeUI.
WDEU 4	Wykonawca musi zaprojektować i wdrożyć w ramach SeUI połączenie z SEOD oraz mechanizm, pozwalający poszczególnym podmiotom wypełniać i aktualizować karty usług z wykorzystaniem danych zawartych w systemie SEOD, tak aby w SeUI nie było konieczne ponowne ręczne wprowadzanie struktury urzędu, danych teleadresowych jednostek urzędu, czy ich godzin pracy. Zaistniałe niezgodności w tym zakresie między danymi w SEOD a SeUI powinny być automatycznie wykrywane i raportowane administratorom (np. gdy w SEOD pojawia się zmiana).
WDEU 5	Wykonawca musi wdrożyć integrację z platformą ePUAP w zakresie przekazywania kart i opisów usług z Portalu e-Uслуг na platformę ePUAP; w wyniku wdrożenia przekazywanie powinno odbywać się w sposób zautomatyzowany (tzn. aktualizacja kart usług na ePUAP następuje automatycznie po aktualizacji w Portalu e-Uслуг, zaś dla opisów usług portalem źródłowym jest ePUAP).
WDEU 6	Dla usług na poziomie 2 i wyższym Wykonawca musi zaprojektować formularze elektroniczne i wdrożyć je na platformie ePUAP dla poszczególnych Partnerów (wg zakresu wskazanego w rozdziale 7.2 „Zakres wdrożenia e-usług”), zaś ich wersje do wydruku i ręcznego wypełnienia w formacie .pdf zamieści w Portalu e-Uслуг.
WDEU 7	Wykonawca musi: <ul style="list-style-type: none"> <li>A) zapewnić, że z odpowiednich stron portalu e-Uслуг poświęconych poszczególnym usługom podmiotów będą bezpośrednie łącza do odpowiednich stron ePUAP z formularzem elektronicznym załatwienia sprawy w danym podmiocie (w zakresie możliwości dawanych przez platformę ePUAP).</li> <li>B) opracować wzory dokumentów elektronicznych, które muszą zgodnie z prawem zostać przekazane do centralnego repozytorium wzorów dokumentów.</li> </ul>
WDEU 8	W zakresie niezbędnym do wdrożenia e-Uслуг na platformie ePUAP oraz integracji z ePUAP : <ul style="list-style-type: none"> <li>A) Wykonawca zobowiązany będzie przekazać poszczególnym Partnerom instrukcję konfiguracji oraz pliki konfiguracyjne przeznaczone do importu (w zależności od decyzji Partnera). Dla tych Partnerów, którzy wyrażą taką wolę i udzielą mu odpowiednich uprawnień</li> <li>B) Wykonawca musi w pełni skonfigurować integrację od strony Platformy</li> </ul>

	<p>ePUAP.</p> <p>C) Jednocześnie wykonawca zobowiązany będzie dostarczyć i zamieścić na portalu CPI w specjalnie przeznaczonym do tego dziale Portalu CPI wszystkie wykorzystywane i opracowane przez siebie pliki konfiguracyjne importowane na platformę ePUAP oraz szczegółowe instrukcje „krok-po-kroku”, umożliwiające administratorom poszczególnych podmiotów samodzielne wgrywanie kolejnych usług oraz zarządzanie istniejącymi, a także zarządzanie i konfigurację integracji.</p>
--	--

## 8.5 Wdrożenie SeUI

	<b>Minimalne wymagania dotyczące procesu wdrożenia produkcyjnego SeUI</b>
	<b>Konfiguracja środowiska produkcyjnego</b>
WP SEUI 1	Po pomyślnym zakończeniu testów funkcjonalnych Systemu, Wykonawca musi przystąpić do konfiguracji środowiska produkcyjnego Systemu.
WP SEUI 2	<p>Wykonawca musi wprowadzić do Systemu ustawienia konfiguracyjne oraz dane niezbędne do normalnej pracy SeUI, w szczególności:</p> <ul style="list-style-type: none"> <li>A) wdrożyć e-usługi publiczne;</li> <li>B) zamieścić w Portalu CPI oraz na Portalu e-Usług wszelkie przewidziane projektem materiały, instrukcje, podręczniki i inne informacje przeznaczone dla administratorów oraz użytkowników Systemu, a związane z funkcjonowaniem i użytkowaniem samego Systemu PSeAP;</li> <li>C) wprowadzić użytkowników i nadać im odpowiednie uprawnienia,</li> <li>D) wdrożyć integrację z ePUAP oraz z innymi komponentami Systemu PSeAP;</li> <li>E) przygotować interfejsy do współpracy z BIP i zewnętrznymi SEOD.</li> </ul>
	<b>Start produkcyjny Systemu</b>
WP SEUI 3	W uzgodnionym z Zamawiającym terminie, Wykonawca musi przeprowadzić procedurę udostępnienia SeUI w sieci Internet.
WP SEUI 4	<p>Po stronie Wykonawcy leży odpowiedzialność za:</p> <ul style="list-style-type: none"> <li>A) Wdrożenie i przetestowanie technicznej dostępności Systemu w sieci Internet (Zamawiający zapewnia domenę i łącze internetowe o przepustowości min. 10 Mbps).</li> <li>B) Dostawę licencji oprogramowania aplikacyjnego Systemu oraz innych licencji oprogramowania niezbędnych do działania Systemu. Wykonawca musi dostarczyć licencje, które zapewnią osiągnięcie następujących parametrów</li> </ul>



	<p>ilościowych konfiguracji Systemu:</p> <ul style="list-style-type: none"> <li>i Zarejestrowanie w Systemie co najmniej 1 000 (tysiąca) aktywnych użytkowników (urzędników - administratorów) korzystających z narzędzi Centralnego Portalu Internetowego oraz systemu CMS (Portal e-Uслуг, podsystemu zarządzania infomatami).</li> <li>ii Brak ograniczeń, które praktycznie mogłyby limitować wielkość Portalu e-Uслуг, liczbę korzystających klientów, liczbę świadczonych e-usług, liczbę JST z województwa Podkarpackiego udostępniających usługi przez SeUI, ograniczać zakres integracji z ePUAP lub w jakikolwiek sposób utrudniać korzystanie z Systemu zgodnie z jego przeznaczeniem.</li> </ul>
WP SEUI 5	Zakończenie procedury startu produkcyjnego oraz pozytywne przejście kompletu testów funkcjonalnych i pozafunkcyjnych (za wyjątkiem testów stabilności opisanych poniżej) przez System jest równoznaczne z rozpoczęciem etapu testów stabilności Systemu.
	<b>Testy stabilności/wydajności Systemu</b>
WP SEUI 6	Podczas etapu testów stabilności, działanie SeUI w trybie normalnej eksploatacji produkcyjnej będzie na bieżąco monitorowane i oceniane pod względem występowania błędów krytycznych lub poważnych.
WP SEUI 7	Etap testów stabilności rozpocznie się wraz ze startem produkcyjnym Systemu.
WP SEUI 8	<p>Zakończenie etapu testów stabilności Systemu nastąpi po podpisaniu protokołów częściowych potwierdzających poniższe zdarzenia:</p> <ul style="list-style-type: none"> <li>A) System działa w trybie normalnej eksploatacji produkcyjnej od co najmniej dwóch miesięcy. W tym okresie serwer ani razu nie zawiesił się i nie wymagał restartu z przyczyn wynikających z błędów oprogramowania, zaś dostępność systemu wyniosła 99% (z wyłączeniem okresów niedostępności, wynikających z przyczyn niezależnych od wykonawcy). W przypadku zawieszenia, konieczności restartu systemu lub wyższej niż 1% niedostępności z winy wykonawcy w ciągu tych 2 miesięcy zamawiający – w zależności od przyczyn i rodzaju problemów – określa o jaki okres, nie dłuższy niż kolejne 2 miesiące, testy stabilności muszą być przedłużone.</li> <li>B) Wszystkie zgłoszone przez Zamawiającego błędy w działaniu oprogramowania Systemu, których status określono jako krytyczny lub poważny, zostały przez Wykonawcę trwale usunięte, a po ich usunięciu wykonano całościowe (kompletne) testy regresywne systemu, które wypadły pomyślnie.</li> <li>C) Żaden nowy błąd ani krytyczny ani poważny dotyczący działania oprogramowania Systemu nie został przez Zamawiającego zgłoszony w ciągu</li> </ul>



---

	<p>ostatnich 30 dni kalendarzowych; w przypadku zgłoszenia takiego błędu okres 30 dni biegnie od nowa, przy czym Zamawiający może ten okres skrócić, w zależności od charakteru i okoliczności zaistniałego błędu oraz czasu i sposobu jego naprawy.</p> <p>D) Pozostałe błędy (inne niż krytyczne i poważne) zostały przez Wykonawcę usunięte.</p>
WP SEUI 9	Na etapie testów stabilności procedury oraz czasy związane z reagowaniem i naprawą błędów oprogramowania oraz rozwiązywaniem problemów sprzętowych są takie same, jak w okresie gwarancji.

## 9 System Elektronicznego Obiegu Dokumentów

W ramach Projektu PSeAP Systemy Elektronicznego Obiegu Dokumentów (SEOD) zostaną dostarczone i wdrożone u 157 Partnerów.

### 9.1 Opis podstawowych wymagań i zakres funkcjonalności

„W” oznacza wymaganie obowiązkowe na moment składania oferty, „D” – wymaganie obowiązkowe wobec systemu docelowego, „O” – wymaganie opcjonalne wobec systemu docelowego.

	Opis podstawowych wymagań i zakres funkcjonalności	Funkcjonalność	Waga
<b>Wymagania</b>	<b>Wymagania ogólne</b>		
SEOD 1	System SEOD musi spełniać wszystkie warunki określone dla systemu EZD w Rozporządzeniu w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14, poz. 67) i wszystkie jego funkcje będą działać zgodnie z tym rozporządzeniem.	W	1
SEOD 2	System SEOD musi realizować pełną funkcjonalność przewidzianą przepisami prawa dla systemu EZD, co pozwoli jednostkom użytkującym ten system wykorzystywać go jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw.	W	1
SEOD 3	Jeśli jakaś czynność kancelaryjna jest obsługiwana przez system (np. dołączenie dokumentu do sprawy), to struktura systemu musi umożliwiać wykonywanie wszystkich wariantów tego zadania dopuszczalnych instrukcją kancelaryjną (np. dołączenie praktycznie dowolnej ilości dokumentów do sprawy – tzn. liczby na tyle dużej, by w praktyce nie napotkać ograniczeń systemu). Zarówno liczba dopuszczalnych dokumentów jak i ich łączny rozmiar powinny być parametrami konfigurowalnymi systemu.	W	1
SEOD 4	Jeśli instrukcja kancelaryjna wprost wskazuje na możliwość automatyzacji jakiegoś zadania w systemie EZD, system SEOD powinien umożliwiać automatyzację tego zadania. Jeśli instrukcja kancelaryjna dopuszcza różne warianty jego wykonania, SEOD powinien zapewniać pełną konfigurowalność sposobu wykonania tego zadania (np. w zakresie rozdziału przesyłek przychodzących, opatrywania przesyłek metadanymi, archiwizacji). System SEOD powinien także umożliwić konfigurowanie maksymalnej wielkości pliku załączanego do sprawy.	W	1



SEOD 5	System SEOD musi umożliwić definiowanie i wykorzystywanie wartości domyślnych dla wybranych pól w formularzach opisujących przesyłki, pisma, dokumenty i sprawy oraz sposób ich przetwarzania, tam gdzie wykorzystanie ustawień domyślnych znacznie usprawni pracę. Ustalenie takiej konfiguracji powinno być możliwe zarówno globalnie dla całego systemu, jak i na poziomie stanowiska lub użytkownika	D	3
SEOD 6	System będzie umożliwiał wykorzystanie skrótów klawiszowych do wywoływania często używanych funkcji. System będzie zawierał zestaw predefiniowanych skrótów klawiszowych i umożliwi zdefiniowanie własnych (nadpisanie predefiniowanych i zdefiniowanie dodatkowych) na poziomie całego systemu oraz pojedynczego użytkownika	D	2
	<b>Rejestracja i rozdział przesyłek</b>		
SEOD 7	System musi obsługiwać rejestrację przesyłek przychodzących w formie papierowej (składane osobiście, przysyłane pocztą) i elektronicznej (składane osobiście na nośnikach, przesyłane przez elektroniczną skrzynkę podawczą oraz pocztą elektroniczną) wraz z załącznikami zgodnie z wymogami Rozporządzenia w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14, poz. 67).	W	1
SEOD 8	W ramach procesu rejestracji przesyłek przychodzących w formie papierowej system musi umożliwić zeskanowanie (z poziomu interfejsu aplikacji) poszczególnych dokumentów, wchodzących w skład przesyłki.	W	1
SEOD 9	System musi umożliwiać skanowanie wsadowe przesyłek (np. przychodzących pocztą).	W	1
SEOD 10	System musi umożliwiać generowanie potwierdzenia przyjęcia przesyłki przychodzącej przez punkt kancelaryjny i opatrzonej kodem kreskowym.	W	1
SEOD 11	System musi umożliwiać rejestrację przesyłek w wielu punktach kancelaryjnych.	W	1
SEOD 12	System musi umożliwiać opatrywanie przesyłek przychodzących metadanymi zgodnie z obowiązującymi przepisami oraz dodatkowymi (konfigurowalny zakres), przy czym metadane powinny być zestawnikowane co najmniej w zakresie rodzaju dokumentu, sposobu dostarczenia oraz danych teleadresowych.	W	1
SEOD 13	System musi umożliwić odróżnienie, jednoznaczną identyfikację i odrębne przetwarzanie (np. niezależne udostępnianie) poszczególnych dokumentów, przechowywanych w postaci skanów, wchodzących w skład przesyłki, przy zachowaniu ich powiązania z przesyłką.	W	1



SEOD 14	System musi umożliwić opcjonalne dodawanie przez użytkownika informacji opisujących poszczególne dokumenty, przesyłki lub sprawy w postaci notatek, zgodnie z Instrukcją Kancelaryjną.	W	1
SEOD 15	Dla dokumentów papierowych nie podlegających skanowaniu oraz dokumentów na nośnikach elektronicznych nie podlegających kopiowaniu do systemu SEOD (wymaganie dotyczy zarówno całych przesyłek, jak i dokumentów wchodzących w skład przesyłki), system musi umożliwić sporządzenie metryki, zawierającej podstawowe informacje o dokumencie (co najmniej – tytuł, identyfikator, notatka).	W	1
SEOD 16	System musi umożliwić prawidłową obsługę przychodzącej poczty elektronicznej, zgodnie z wymogami przepisów w zakresie instrukcji kancelaryjnych (rejestracja w rejestrze przesyłek wpływających lub bezpośrednie dołączenie wiadomości z załącznikami do akt sprawy); w sposób niezależny od użytkowanego programu pocztowego.	W	1
SEOD 17	System musi automatycznie pobierać przesyłki, które przysły przez elektroniczną skrzynkę podawczą systemu ePUAP, i musi umożliwić ich rejestrację w systemie w trybie półautomatycznym, automatycznym lub ręcznym, w zależności od konfiguracji.	W	1
SEOD 18	Dla przesyłek, które przysły przez elektroniczną skrzynkę podawczą systemu ePUAP, system SEOD musi umożliwić realizację rozdziału w sposób automatyczny (w zależności od kategorii usługi), półautomatyczny (dane wypełniane automatycznie, wymagane zatwierdzenie) lub ręczny, w zależności od konfiguracji.	D	5
SEOD 19	Rozdział przesyłek przychodzących do właściwych komórek merytorycznych musi się odbywać poprzez przekazanie uprawnień do plików i informacji zawartych w systemie.	W	1
SEOD 20	System musi umożliwić generowanie i drukowanie nalepek z kodami kreskowymi na dokumenty papierowe oraz nośniki i odnajdywanie na podstawie zeskanowanej nalepki odwzorowania cyfrowego bądź metryki danego dokumentu.	W	1
SEOD 21	System musi umożliwić rejestrację obiegu (lokalizacja, czas przemieszczenia, użytkownik) dokumentów papierowych (dla których istnieje odwzorowanie cyfrowe oraz dla których nie zostało ono wykonane) oraz nośników.	W	1
SEOD 22	System musi posiadać interfejsy, umożliwiające automatyczne przekazanie przesyłek przychodzących przez ePUAP bezpośrednio do ewentualnych podłączonych systemów dziedzinowych (bez rejestracji w rejestrze przesyłek przychodzących). SEOD umożliwi skonfigurowanie warunków automatycznego przekazywania przesyłek pochodzących ePUAP do innych systemów.	D	7



SEOD 23	System musi posiadać zestandaryzowane (tzn. określone i możliwe do zastosowania dla wielu systemów dziedzinowych) interfejsy oparte o język XML, umożliwiające automatyczne pobieranie z systemów dziedzinowych dokumentów do wysyłki wraz z danymi niezbędnymi do wysyłki. Dostosowanie systemów dziedzinowych do współpracy nie jest zadaniem Wykonawcy.	D	6
	<b>Skanowanie dokumentów</b>		
SEOD 24	System musi umożliwić sporządzanie odwzorowań cyfrowych dokumentów poprzez skanowanie dostępne z poziomu aplikacji SEOD, zgodnie z wymaganiami określonymi w instrukcji kancelaryjnej.	W	1
SEOD 25	System musi umożliwiać wykonanie OCR w języku polskim dla skanowanych dokumentów i jego wykorzystanie w późniejszym przetwarzaniu sprawy lub przeszukiwaniu pełnotekstowym dokumentów (dotyczy pisma maszynowego a nie odręcznego).	W	1
SEOD 26	Narzędzie OCR poprawnie rozpozna 90% wyrazów w załączonym dokumencie testowym oraz zachowa układ strony i tabeli (wzór dokumentu zawiera Załącznik 3).	D	2
	<b>Procedowanie pism i spraw</b>		
SEOD 27	System musi umożliwić rejestrację, przechowywanie, procedowanie oraz dołączanie do akt sprawy dokumentów elektronicznych, dokumentów papierowych w postaci odwzorowań, jak również metryk (dla dokumentów papierowych nie skanowanych i elektronicznych na nośnikach).	W	1
SEOD 28	System musi umożliwić wszczynanie, prowadzenie i załatwianie spraw, przechowywanie akt sprawy i prowadzenie spisów spraw zgodnie z obowiązującymi przepisami. System automatycznie musi nadawać znak sprawy i zapewnia jego zgodność z wymogami instrukcji kancelaryjnej.	W	1
SEOD 29	System musi umożliwiać ręczne przenie numerowanie sprawy wyłącznie w przypadkach dopuszczonych instrukcją kancelaryjną.	W	1
SEOD 30	System musi umożliwić prowadzenie rejestrów kancelaryjnych, w tym rejestru przesyłek wpływających, wychodzących oraz pism wewnętrznych, definiowanie i prowadzenie dowolnych innych rejestrów kancelaryjnych dopuszczonych instrukcją kancelaryjną.	W	1
SEOD 31	System musi umożliwić numerację i klasyfikację pism oraz spraw w oparciu o JRWA zgodnie z instrukcją kancelaryjną.	W	1
SEOD 32	System musi od strony technicznej umożliwić stworzenie odrębnych podrzędnych SEOD dla jednostek podległych, z odrębnym JRWA i odrębną hierarchią użytkowników.	D	12



SEOD 33	System musi umożliwić i procedowanie i dekretację spraw oraz pism z wykorzystaniem mechanizmu procedowania według definiowalnych ścieżek (mechanizm przepływu pracy — workflow) w pełni zgodnie z instrukcją kancelaryjną.	W	1
SEOD 34	System musi umożliwić akceptację dokumentów z wykorzystaniem mechanizmu procedowania według zdefiniowanych ścieżek (mechanizm przepływu pracy — workflow) w pełni zgodnie z instrukcją kancelaryjną. System obsługuje akceptację jedno – lub wielostopniową.	W	1
SEOD 35	Akceptacja pism elektronicznych przeznaczonych do wysyłki musi się odbywać z wykorzystaniem podpisu elektronicznego zgodnie z wymogami prawa. System musi zapewniać integralność, rozliczalność i niezaprzeczalność treści, które zostały zaakceptowane.	W	1
SEOD 36	System musi umożliwić zapis projektów pism przekazywanych pomiędzy użytkownikami lub komórkami w trakcie załatwiania sprawy, a także zamieszczanie adnotacji odnoszących się do projektów pism.	W	1
SEOD 37	System musi zapewnić prowadzenie i wydruk metryki sprawy zgodnie z obowiązującymi przepisami.	W	1
SEOD 38	System musi umożliwić opisywanie spraw i akt sprawy metadanymi zgodnie z obowiązującymi przepisami.	W	1
SEOD 39	System musi umożliwić dokumentowanie wyjęcia dokumentacji ze składu chronologicznego lub ze składu informatycznych nośników danych.	D	3
SEOD 40	SEOD ma umożliwiać wiązanie dowolnych dokumentów ze sobą oraz ze sprawami oraz dodawanie konfigurowalnych atrybutów (opisów, notatek) do tych powiązań.	D	3
	<b>Przeszukiwanie danych, raporty i zestawienia</b>		
SEOD 41	System musi umożliwić sporządzanie i wydruk raportów, statystyk i zestawień, w szczególności wymaganych przepisami prawa. System umożliwi monitorowanie liczby spraw i terminowości ich załatwiania (globalnie, przez poszczególne komórki i osoby) w zadanych przedziałach czasu, także w podziale na kategorie spraw. Możliwość generowania raportów będzie zależna od uprawnień i będzie dotyczyła pracy osób i komórek podległych oraz pracy osoby sporządzającej raport.	W	1
SEOD 42	System musi umożliwić sporządzenie raportu w postaci pliku .pdf, .xls, .rtf, .csv, .xml, .html, *.doc, *.odt	W	1
SEOD 43	System musi umożliwić definiowanie raportów cyklicznych, przesyłanych na zadany adres e-mail.	W	1
SEOD 44	System musi umożliwić przeszukiwanie i sortowanie pism i spraw według złożonych kryteriów, w szczególności wg znaku sprawy, identyfikatora przesyłki, osoby lub komórki odpowiedzialnej, kategorii JRWA, dat wpłynięcia lub	W	1



	załatwienia, terminu załatwienia, statusu pisma lub sprawy, danych klienta urzędu, nadawcy, adresata.		
SEOD 45	System musi umożliwić użytkownikowi dostęp do: zestawienia spraw, za które jest odpowiedzialny, zestawienia aktualnych zadań wynikających z przepływu pracy (sprawy i korespondencja, w odniesieniu do których użytkownik ma aktualnie coś do zrobienia), zestawienia korespondencji otrzymanej i wysłanej w podziale na korespondencję wewnętrzną i z podmiotami zewnętrznymi	W	1
SEOD 46	System musi umożliwić pełnotekstowe przeszukiwanie dokumentów w obrębie wyszukanego wcześniej zbioru, w tym co najmniej dokumentów w formatach .txt, .pdf (zawierający tekst), rtf, .doc, .odt, .docx.	D	3
	<b>Korespondencja wychodząca</b>		
SEOD 47	System musi posiadać funkcję automatycznej wysyłki pism za potwierdzeniem odbioru przez platformę ePUAP.	W	1
SEOD 48	Jeśli będzie to technicznie możliwe od strony platformy ePUAP na dzień odbioru Systemu, System musi odbierać z platformy ePUAP informację zwrotną o doręczeniu przesyłki – Urzędowe Poświadczenie Doręczenia i automatycznie musi ją skierować do właściwego użytkownika.	D	3
SEOD 49	System musi umożliwić automatyczną wysyłkę korespondencji pocztą elektroniczną poprzez pobranie adresu odbiorcy i wysłanie treści pisma w treści poczty oraz załączników w formie załączników do poczty.	D	5
SEOD 50	System musi umożliwić odnotowanie wysyłki wszelkich przesyłek wychodzących w rejestrze i opatrzenie ich metadanymi zgodnie z przepisami. SEOD będzie w miarę możliwości automatyzował te czynności.	W	1
SEOD 51	SEOD musi umożliwić generowanie korespondencji seryjnej i automatyzację jej wysyłki (do zdefiniowanych, konfigurowalnych grup odbiorców).	W	1
	<b>E-formularze i generowanie pism</b>		
SEOD 52	SEOD musi umożliwić używanie i wyświetlanie w obrębie systemu formularzy („e-formularze SEOD”) do wypełnienia oraz dawać możliwość wykorzystania pól z tych formularzy do tworzenia szablonów (e-szablony SEOD).	O	3
SEOD 53	SEOD musi umożliwić wykorzystywanie e-szablonów SEOD na ścieżce przetwarzania sprawy: użytkownik wypełnia e-szablon danymi, generując w ten sposób e-dokument SEOD. Na podstawie wyświetlonego i zatwierdzonego przez użytkownika e-dokumentu system musi generować pismo do wysyłki.	O	3
SEOD 54	SEOD musi umożliwić przechowywanie, przeszukiwanie i wersjonowanie e-szablonów, ich współdzielenie między użytkownikami oraz nadawanie uprawnień do ich modyfikacji.	O	3





SEOD 55	Pismo do wysyłki wygenerowane na podstawie e-szablону mus być w formacie edytowalnym (co najmniej *.doc, *.odt, *.rtf).	O	5
	<b>Archiwizacja</b>		
SEOD 56	SEOD musi zapewnić automatyczne przejmowanie dokumentacji przez archiwum zakładowe po upływie okresu przewidzianego w instrukcji kancelaryjnej. Przejęcie dokumentacji musi polegać na przekazaniu archiwistce uprawnień do tej dokumentacji w systemie SEOD i ograniczeniu uprawnień komórki merytorycznej, zgodnie z instrukcją kancelaryjną.	W	1
SEOD 57	System SEOD musi posiadać dedykowane funkcje do udostępniania i wycofywania dokumentacji elektronicznej z archiwum zakładowego.	W	1
SEOD 58	SEOD musi posiadać funkcje wspierające proces porządkowania dokumentacji w archiwum zakładowym (wskazanie dokumentacji wymagającej uzupełnienia).	D	1
SEOD 59	System musi realizować brakowanie akt elektronicznych oraz przekazanie akt do archiwum państwowego oraz musi umożliwić sporządzenie i przechowywanie odpowiedniej dokumentacji. SEOD musi wspierać pracę archiwisty poprzez automatyczne typowanie dokumentacji do brakowania lub przekazania do archiwum państwowego (po upływie terminów związanych z danymi kategoriami archiwalnymi) oraz funkcjonalność automatycznych przypomnień	W	1
SEOD 60	System musi zapewnić wsparcie dla procesu archiwizacji informatycznych nośników danych oraz dokumentów papierowych dla których nie wykonano pełnego odwzorowania cyfrowego, w tym umożliwi: A) sporządzanie spisu zdawczo-odbiorczego, B) zapis miejsca ich przechowywania i kategorii archiwalnej, C) wsparcie procedury brakowania akt, wypożyczeń oraz przekazania do archiwum państwowego poprzez odnotowywanie tych zdarzeń, sporządzanie i przechowywanie odpowiedniej dokumentacji.	D	6
	<b>Opłaty</b>		
SEOD 61	System musi przechowywać informacje o opłatach i umożliwi uzależnienie czynności na ścieżce sprawy od wniesienia opłat.	D	2
SEOD 62	System musi umożliwić wnoszenie opłat przez ePUAP oraz automatyczne pozyskiwanie informacji o wniesionych w ten sposób opłatach i wykorzystywanie jej do procedowania dokumentów i spraw.	D	5
SEOD 63	System musi umożliwić wprowadzanie informacji o otrzymanych przelewach ręcznie przez urzędników obsługujących sprawę lub w postaci zaimportowanego dokumentu XML, umożliwia użytkownikom identyfikację	D	3





	przelewów (tzn. wiązanie przelewów ze sprawami) i – tam gdzie to możliwe – automatycznie identyfikuje przelewy lub podpowiada ich identyfikację w oparciu o konfigurowalne reguły.		
SEOD 64	System musi być przygotowany na współpracę z systemem finansowo-księgowym w zakresie automatycznego pozyskiwania informacji o opłatach wniesionych w kasie lub przelewem (SEOD udostępni odpowiedni interfejs integracyjny – co najmniej Web Services oraz wymiana danych przez plik XML).	D	7
	<b>Przepływ pracy (workflow)</b>		
SEOD 65	System musi umożliwić definiowanie ścieżek dla korespondencji i spraw w oparciu o strukturę instytucji oraz powiązanie ścieżki z daną kategorią spraw. Ścieżki muszą określać :warunki (w tym dokumenty) wymagane do rozpoczęcia, kontynuacji i zakończenia procedowania, czynności do wykonania i terminy dla poszczególnych kroków przetwarzania sprawy lub korespondencji, stanowiska odpowiedzialne za ich wykonanie.	W	1
SEOD 66	Ścieżki muszą dopuszczać rozwidlanie oraz łączenie się podścieżek (ścieżek w obrębie innych ścieżek).	W	1
SEOD 67	System musi umożliwić tworzenie i obsługę podścieżek, w szczególności musi umożliwić użytkownikowi procedującemu korespondencję lub sprawę zdefiniowanie podścieżki, która zaczyna się i kończy w jego węźle.	D	2
SEOD 68	Ścieżki mogą zawierać także warunki określone dla dokumentów XML wymaganych na dowolnym etapie sprawy (np. wariant ścieżki uruchamiany jest w zależności od zawartości jednego z pól wniosku).	D	2
SEOD 69	System musi umożliwić import, eksport i wykorzystanie schematów ścieżek. Schematy ścieżek są to ścieżki, które nie zawierają struktury stanowisk, lecz jedynie wybrane elementy związane z przetwarzaniem spraw, np. terminy, czynności, wymagane dokumenty i opłaty, warunki procedowania, e-formularze SEOD.	O	5
SEOD 70	System musi umożliwić zamieszczanie na węzłach ścieżki opisu zadań do wykonania oraz e-formularzy SEOD służących do przygotowania przez urzędnika dokumentów elektronicznych. Formularze muszą umożliwiać wypełnianie automatycznie zdefiniowanymi danymi z wniosku interesanta lub z systemów zewnętrznych (w przypadku integracji z systemami centralnymi i dziedzinowymi).	D	2
SEOD 71	System, we współpracy z systemem ePUAP, musi umożliwić automatyczne i ręczne(w tym z podpowiedzią) sprawdzanie informacji w rejestrach centralnych (jak np. PESEL) i wykorzystywanie uzyskanych w ten sposób informacji jako	D	3



	warunków przy procedowaniu spraw i pism.		
SEOD 72	System musi zapewnić przydzielanie spraw i korespondencji, przekazanych na dane stanowisko, konkretnym użytkownikom, pracującym na tym stanowisku.	W	1
SEOD 73	System musi umożliwić przekazywanie korespondencji/sprawy na stanowisko lub bezpośrednio do wskazanego Użytkownika.	W	1
SEOD 74	System musi umożliwić ewidencjonowanie i wersjonowanie ścieżek obiegu.	W	1
SEOD 75	System musi umożliwić podgląd historii sprawy, ścieżki obiegu sprawy (w formie grafu).	W	1
SEOD 76	System musi umożliwić procedowanie sprawy lub korespondencji trybem „ad hoc” poprzez określanie na bieżąco kolejnych stanowisk zajmujących się sprawą/korespondencją bez wykorzystywania uprzednio zdefiniowanych ścieżek procedowania sprawy/korespondencji. Użytkownik może przejść do trybu „ad hoc” w dowolnym momencie przetwarzania sprawy/korespondencji.	W	1
SEOD 77	System musi umożliwić modelowanie ścieżek w narzędziu graficznym.	W	1
SEOD 78	System musi umożliwić tworzenie ścieżek obiegu na podstawie historii obiegu pisma lub sprawy; w szczególności dotyczy to obiegu trybem „ad hoc”.	D	2
SEOD 79	SEOD musi umożliwić wersjonowanie, przechowywanie i zarządzanie e-formularzami SEOD w sposób niezależny od ścieżek, z którymi są one powiązane. System musi umożliwić także śledzenie powiązań e-formularzy i e-formularzy SEOD ze ścieżkami.	D	2
SEOD 80	System musi umożliwić tworzenie i modyfikację e-formularzy z wykorzystaniem podsystemu formularzy wchodzącego w skład CPI, wykorzystanie e-formularzy udostępnianych poprzez CPI.	D	4
SEOD 81	System musi umożliwić monitorowanie i kontrolę obiegu dokumentów z wykorzystaniem konfigurowalnych raportów, zestawień, statystyk i alertów – w zakresie pracy własnej oraz osób podległych.	D	7
SEOD 82	System musi umożliwić przypisywanie (w ramach ścieżki lub „ad-hoc”) procesom i zadaniom terminów realizacji, monitorowanie terminowości ich realizacji, automatyczne konfigurowalne przypomnienia i alerty.	D	2
	<b>Wsparcie organizacji pracy</b>		
SEOD 83	System musi posiadać funkcjonalność kalendarza i zadań (z terminami i priorytetami) oraz notatek dla użytkowników.	D	3
SEOD 84	System musi umożliwić obsługę wielu kalendarzy z możliwością ich łącznego udostępniania w terminarzu użytkownika, włączania i wyłączania subskrypcji i podglądu wybranych kalendarzy.	D	4



SEOD 85	Dostęp do kalendarzy musi być regulowany przez system uprawnień do ich tworzenia, edycji, publikowania, podglądu i subskrypcji.	D	3
SEOD 86	System musi umożliwiać definiowanie zdarzeń kalendarza i zadań dla innych osób oraz ich grup przez osoby uprawnione (np. przełożonego dla podwładnych).	D	4
SEOD 87	Kalendarz musi umożliwiać podgląd zadań w siatce o rozdzielczości co najmniej 15 minut, zaś ich definiowanie z dokładnością do 5 minut.	D	2
SEOD 88	System musi być wyposażony w funkcjonalność komunikatora tekstowego. Komunikator musi być wewnętrznym oprogramowaniem dla urzędu i nie może umożliwiać komunikacji z zewnętrznymi komunikatorami dostępnymi publicznie.	D	5
SEOD 89	System musi umożliwić użytkownikowi podgląd przypisanych do niego spraw i korespondencji, z możliwością sortowania, filtrowania i przeszukiwania.	D	5
SEOD 90	System musi umożliwić nadawanie priorytetów pismom i sprawom	D	5
SEOD 91	SEOD musi umożliwić współpracę z urządzeniami mobilnymi zgodnie z polityką bezpieczeństwa stosowaną u danego Partnera. Współpraca z urządzeniem mobilnym wymaga dostosowania rozwiązania do rozdzielczości ekranu danego typu urządzenia. SEOD musi udostępnić narzędzia administracyjne, umożliwiające zdefiniowanie zasad w tym zakresie, co najmniej: zezwolenie na korzystanie z urządzeń mobilnych spoza sieci urzędu dla wybranych użytkowników (domyślnie uprawnienie to musi być zablokowane dla wszystkich), definiowanie dla tych użytkowników dopuszczonych dni i godzin pracy, listy dopuszczonych urządzeń, a także dopuszczonych form logowania do SEOD (karta kryptograficzna, login i hasło, profil zaufany). Korzystanie z SEOD spoza sieci urzędu musi być możliwe wyłącznie z wykorzystaniem bezpiecznego połączenia VPN.	O	8
	<b>Podpisywanie dokumentów</b>		
SEOD 92	System musi umożliwić składanie i weryfikowanie podpisu elektronicznego na każdym dokumencie elektronicznym w dowolnej liczbie podpisów elektronicznych różnych rodzajów: podpis profilem zaufanym ePUAP, bezpieczny podpis elektroniczny z wykorzystaniem certyfikatów kwalifikowanych jak i niekwalifikowanych, w tym weryfikacja podpisów z listy TSL.	W	1
SEOD 93	Do weryfikacji podpisu elektronicznego system musi korzystać z funkcjonalności platformy ePUAP, przy czym powinna ona być możliwa do wywołania dla dowolnego dokumentu w systemie na żądanie użytkownika.	W	1

SEOD 94	System musi umożliwić pobieranie, przechowywanie i dostęp do archiwalnej wersji podpisu elektronicznego wykonanej przy składaniu dokumentu przez platformę ePUAP.	D	4
	<b>Integracja z ePUAP:</b>		
SEOD 95	System musi przyjmować dokumenty elektroniczne złożone przez klientów za pośrednictwem platformy ePUAP i umożliwiać automatyczne kierowanie ich na właściwą ścieżkę zgodnie z e-usługą, której dotyczą	W	1
SEOD 96	System musi umożliwiać użytkownikom pobieranie informacji o płatnościach dokonanych przez ePUAP. System musi umożliwiać integrację z ePUAP w zakresie realizacji płatności dokonywanych przez interesantów.	D	3
SEOD 97	System musi umożliwiać doręczanie dokumentów poprzez ePUAP.	W	1
SEOD 98	System musi być zintegrowany z ePUAP w zakresie słowników.	W	1
SEOD 99	System musi być zintegrowany z ePUAP w zakresie uwierzytelniania (SSO) oraz weryfikacji podpisu elektronicznego z wykorzystaniem profilu zaufanego, bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym lub niekwalifikowanym certyfikatem.	D	3
SEOD 100	System musi być zintegrowany z ePUAP w zakresie funkcji bezpieczeństwa, związanych z podpisem cyfrowym (weryfikacja bezpiecznego podpisu elektronicznego, znakowanie czasem, sporządzanie archiwalnej wersji podpisu elektronicznego na żądanie użytkownika z SEOD) w zakresie, w jakim umożliwi to ePUAP	D	3
	<b>Integracja ze stronami podmiotowymi BIP:</b>		
SEOD 101	System musi umożliwić publikację dowolnych dokumentów (w tym również związanych z funkcjonowaniem Biura Rady) na stronach podmiotowych poprzez opracowany w tym celu interfejs udostępniony poprzez Web Services, wymianę przez pliki, JMS (Wykonawca nie ma obowiązku dostosować zewnętrznych systemów BIP do korzystania z tych usług).	D	5
SEOD 102	System musi posiadać wbudowany edytor aktów prawnych. Proces przygotowania i publikacji aktu prawnego musi obejmować przygotowanie wersji roboczej oraz jej akceptację, która może lecz nie musi obejmować podpisanie aktu prawnego bezpiecznym podpisem elektronicznym weryfikowanym kwalifikowanym certyfikatem. Akt prawny jest po akceptacji automatycznie eksportowany do systemu zewnętrznego obsługującego publikację (dziennik urzędowy).	D	6
SEOD 103	System musi umożliwić informowanie o statusie sprawy na stronach podmiotowych poprzez opracowany w tym celu interfejs udostępniony poprzez Web Services, wymianę przez pliki, JMS (Wykonawca nie ma obowiązku dostosować zewnętrznych systemów BIP do korzystania z tych usług) na	D	5

	podstawie numeru sprawy. System musi także umożliwić informowanie o statusie sprawy poprzez system CMS (Portal e-Uslug) na podstawie identyfikacji i uwierzytelnienia w Portalu e-Uslug.		
	<b>Obsługa zastępstw:</b>		
SEOD 104	System musi umożliwić wprowadzanie zmian kadrowych, urlopów i zastępstw bez konieczności modyfikacji ścieżek procedowania i umożliwia przekazanie osobie zastępującej części lub całości uprawnień osoby zastępowanej. Uprawnienia muszą być przekazane na określony czas dat lub bezterminowo.	W	1
SEOD 105	Funkcjonalność obsługi zastępstw, zmian kadrowych i urlopów umożliwia ustalenie, która osoba faktycznie realizowała daną czynność w systemie (każdy z użytkowników zachowuje swoją tożsamość i działa w oparciu o swoje konto użytkownika).	W	1
	<b>Administracja systemem SEOD i bezpieczeństwo</b>		
SEOD 106	System musi umożliwić ewidencjonowanie struktury instytucji oraz jej pracowników, które umożliwią przypisanie pracowników (osób) do stanowisk (funkcji).	W	1
SEOD 107	System musi umożliwić definiowanie uprawnień, w tym delegowanie części lub całości posiadanych uprawnień.	W	1
SEOD 108	System umożliwi zarządzanie uprawnieniami w oparciu o grupy uprawnień i grupy zasobów, jakich dotyczą. System uprawnień musi być zdolny do odzwierciedlenia uprawnień i odpowiedzialności poszczególnych urzędników, stosowany w jednostkach samorządu terytorialnego i wynikający z Instrukcji Kancelaryjnych oraz struktury stanowisk.	W	1
SEOD 109	System musi umożliwić definiowanie sposobu logowania dla poszczególnych użytkowników i grup użytkowników. Dostępne muszą być co najmniej następujące metody logowania: użytkownik/hasło, karta kryptograficzna, jednokrotne logowania przez domenę, profil zaufany, Single Sign-On na podstawie danych użytkownika platformy ePUAP.	D	2
SEOD 110	Przy logowaniu system musi prezentować użytkownikowi informację o dacie i czasie ostatniego udanego logowania oraz ostatniego nieudanego logowania.	D	1
SEOD 111	System musi także umożliwiać generowanie raportu dotyczącego logowań użytkownika (przez użytkownika i administratora) oraz wykrywać zachowania określone jako podejrzane i uruchamiać konfigurowalne alerty w tym zakresie. Konfiguracja powinna dotyczyć tego, kto ma być informowany (np. użytkownik, administrator), w jakich przypadkach, w jakiej formie (np. sms, mail, alert w systemie).	D	2
SEOD 112	Hasła są przechowywane w systemie w formie zaszyfrowanej i nie ma możliwości ich odtworzenia, lecz jedynie zresetowania. Po zresetowaniu hasła użytkownika przez	W	1

	administradora system zmusza użytkownika do zdefiniowania nowego hasła przy pierwszym logowaniu.		
SEOD 113	System umożliwia administratorowi wymuszenie okresowej zmiany haseł (i zdefiniowanie odpowiedniego interwału czasowego) oraz wspiera wykrywanie kont nieużywanych poprzez odpowiednie alerty.	D	2
SEOD 114	System musi umożliwić wykonywanie kopii bezpieczeństwa (backup) z wykorzystaniem dostarczonego w tym celu sprzętu. System musi umożliwić automatyzację wykonywania backupu w określonych interwałach czasu lub pod określonymi warunkami i umożliwia ustawienie częstotliwości backupu. Zaoferowane rozwiązanie musi być zdolne do tworzenia kopii zapasowych (backupu) danych dokonywanych nie rzadziej niż codziennie.	W	1
SEOD 115	System powinien umożliwiać tworzenie backupu pełnego, backupu różnicowego i backupu przyrostowego. Wykonawca musi opisać procedurę backupu.	W	1
SEOD 116	System musi umożliwić zapis wszystkich czynności wykonywanych w systemie przez jego użytkowników, z możliwością jednoznacznego wskazania użytkownika, który wykonał daną czynność (rozliczalność). Przy usuwaniu rekordów z danymi osobowymi zgodnie z ustawą o danych osobowych, System zapewnia zachowanie pozostałych informacji o użytkowniku i jego aktywności historycznej, a także dokumentów związanych z użytkownikiem.	W	1
SEOD 117	System musi zapewnić bezpieczeństwo komunikacji z systemami zewnętrznymi w szczególności poprzez mechanizm podpisu cyfrowego i szyfrowanie komunikacji. Administrator musi dysponować interfejsem do nadawania uprawnień integrowanym aplikacjom.	D	2
	<b>Słowniki i ewidencje</b>		
SEOD 118	Zakres wartości w słownikach prowadzonych przez system powinien być konfigurowalny przez administratora lub pochodzić z rejestrów centralnych (np. TERYT). Zmiana wartości w słownikach nie może powodować zmian w dokumentach sporządzonych z wykorzystaniem poprzednich wersji słowników.	W	1
SEOD 119	System musi umożliwić prowadzenie: Ewidencji Klientów Urzędu – EKU zawierającej ewidencję osób fizycznych oraz prawnych (z wyróżnieniem JST). Ewidencje te powinny zawierać dane identyfikacyjne i teleadresowe. Dla rejestrowanej sprawy muszą być wprowadzane odnośniki do Ewidencji Klientów Urzędu. Dla Ewidencji Osób Fizycznych system musi umożliwić generowanie raportu danych osobowych zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych	W	1



	i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji generowania raportu danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024).		
SEOD 120	System musi umożliwić prowadzenie książki teleadresowej interesantów i wspiera wykorzystywanie jej w procesie rejestracji i wysyłce przesyłek, tworzeniu pism, rejestracji spraw. System musi umożliwić definiowanie wielu adresów (co najmniej do 5) dla interesanta, a także odrębne oznaczenie adresu zameldowania, zamieszkania, korespondencyjnego. Zmiana danych w książce teleadresowej nie może pociągać za sobą zmian we wcześniejszych dokumentach (także wpisach w systemie) związanych z interesantem.	W	1
SEOD 121	System musi umożliwiać tworzenie grup interesantów (np. poprzez dodatkowe atrybuty) na podstawie książki teleadresowej i z nią zsynchronizowanej. Grupy będą wykorzystywane do wyszukiwania i korespondencji seryjnej.	D	5
SEOD 122	System musi umożliwić nadawanie i ograniczanie uprawnień do danych osobowych interesantów – osób fizycznych, zapewniając ochronę tych danych zgodnie z ustawą o ochronie danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024).	W	1
SEOD 123	Słowniki prowadzone i wykorzystywane w systemie muszą obejmować w szczególności: słownik dekretacji, słownik lokalizacji, słownik rodzajów nośników, słownik kategorii archiwalnych, JRWA.	W	1
SEOD 124	System musi umożliwić zdefiniowanie dodatkowych metadanych do opisu spraw, akt sprawy, przesyłek wchodzących i wychodzących oraz dowolnych dokumentów.	W	1
SEOD 125	System musi umożliwić zdefiniowanie dodatkowych słowników.	W	1
	<b>Inne</b>		
SEOD 126	System musi posiadać wewnętrzny edytor, służący do sporządzania notatek, załączanych do akt sprawy.	W	1
SEOD 127	System musi umożliwiać przeszukiwanie zawartości archiwów utworzonych w formatach: ZIP, TAR, GZIP, 7z.	D	2
SEOD 128	System musi umożliwić wysyłanie i odbieranie faksów z poziomu interfejsu użytkownika wewnętrznego.	D	2
	<b>Akty prawne</b>		
SEOD 129	Wymaga się aby z poziomu SEOD był dostępny Edytor Aktów Prawnych XML zgodny z: A) Ustawą z 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (jednolity tekst Dz. U z 2011 r. Nr 197, poz. 1172).	W	1





	<p>B) Rozporządzeniem Prezesa Rady Ministrów z dnia 27 grudnia 2011 r. w sprawie wymagań technicznych dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne, dzienników urzędowych wydawanych w postaci elektronicznej oraz środków komunikacji elektronicznej i informatycznych nośników danych (Dz.U. z 2011r. Nr 289, poz. 1699)</p> <p>C) Rozporządzeniem Prezesa Rady Ministrów z dnia 3 października 2011 r. w sprawie określenia wzoru graficznego winiety dzienników urzędowych oraz pierwszej i ostatniej strony Dziennika Urzędowego Rzeczypospolitej Polskiej „Monitor Polski B”, a także wzoru okładek i strony tytułowej załączników do tego dziennika urzędowego (Dz. U. z 2011 r. Nr 214, poz. 1269) .</p> <p>D) Rozporządzeniem Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz.U. Nr 100, poz.908).</p>		
SEOD 130	System musi umożliwiać utworzenia nowego projektu aktu prawnego, edycję wcześniej zapisanego aktu prawnego, podpisanie aktu prawnego w Edytorze XML bezpośrednio z poziomu SEOD.	W	1
SEOD 131	System musi umożliwiać przekazywanie do publikacji podpisanych (uchwalonych) aktów prawnych z poziomu SEOD do Dziennika Urzędowego.	W	1
SEOD 132	System musi umożliwiać automatyczne generowanie tekstów ujednoliconych i historycznych dla każdej zmiany aktu.	W	1
SEOD 133	System musi posiadać możliwość utworzenia nowego projektu aktu prawnego, edycję wcześniej zapisanego aktu prawnego, podpisanie aktu prawnego w Edytorze XML bezpośrednio z poziomu SEOD.	W	1
SEOD 134	System musi umożliwiać przekazywanie do publikacji podpisanych (uchwalonych) aktów prawnych z poziomu SEOD do Dziennika Urzędowego.	W	1
SEOD 135	System musi umożliwiać tworzenie aktu prawnego w edytorze wzorowanym na popularnych edytorach biurowych (np. MS Word).	W	1
SEOD 136	<p>System musi umożliwiać automatyczne tworzenie aktu w formacie XML na podstawie dokumentów przygotowanych w innych edytorach tekstów:</p> <p>A) Możliwość „wklejenia” kompletnej treści aktu prawnego do edytora(wbudowanego w SEODSWOD) z aplikacji Microsoft Word oraz OpenOffice.org Writer wraz z wszystkimi załącznikami graficznymi i tabelami,</p> <p>B) Automatyczne rozpoznawanie jednostek redakcyjnych użytych w przeklejonym dokumencie i ich konwersja</p>	W	1





	do formatu XML		
SEOD 137	<p>System musi umożliwiać ręczne tworzenie aktu prawnego bezpośrednio w edytorze:</p> <ul style="list-style-type: none"> <li>A) Tworzenie aktu w widoku strony (identycznie jak w przypadku popularnych programów biurowych do edycji tekstu),</li> <li>B) Wbudowana logika rozpoznająca poszczególne jednostki redakcyjne i pozwalająca na automatycznie numerowanie poszczególnych jednostek,</li> <li>C) Obsługa wszystkich jednostek redakcyjnych: <ul style="list-style-type: none"> <li>i Jednostki podstawowe: Metryka, Preambuła;</li> <li>ii Jednostki systematyzacyjne wyższego rzędu: Część, Księga, Tytuł, Dział, Rozdział, Oddział, Podstawowe;</li> <li>iii Jednostki redakcyjne: Artykuł, Paragraf, Ustęp, Punkt, Litera, Tiret;</li> <li>iv Elementy redakcyjne: Akapit, Śródtytuł, Przypis, Uzasadnienie;</li> <li>v Elementy potomne: Podpis, Organ poświadczający;</li> <li>vi Elementy niestandardowe (dodatkowe): Wielka litera, Cyfra rzymska, Podział strony;</li> <li>vii Zasoby: Obraz , Tabela, Załącznik, Załącznik binarny, Link, Link do podstawy prawnej (powiązanie automatyczne), Wyspa, Uzasadnienie;</li> </ul> </li> <li>D) Podstawowe opcje formatowania: <ul style="list-style-type: none"> <li>i Wytłuszczenie</li> <li>ii Kursywa</li> <li>iii Podkreślenie</li> <li>iv Indeks górny</li> <li>v Indeks dolny</li> <li>vi Wstawianie symboli</li> <li>vii Zmiana numeracji jednostki redakcyjnej</li> <li>viii Przenumerowanie całości aktu</li> <li>ix Orientacja strony</li> </ul> </li> <li>E) Szablony formatowania – możliwość zdefiniowania dowolnego szablonu formatowania pozwalającego na określenie sposobu formatowania każdej jednostki redakcyjnej w zakresie: <ul style="list-style-type: none"> <li>i Rodzaju czcionki i jej wielkości,</li> <li>ii Wcięcie i akapitów,</li> <li>iii Sposobu numerowania (cyfry rzymskie / arabskie),</li> <li>iv Prefiksu dla danego elementu,</li> <li>v Obsługa niestandardowych metryk dla aktów prawnych – rozstrzygnięcie nadzorcze, decyzja administracyjna, wyrok,</li> <li>vi Możliwość wyłączenia metryki aktu i zdefiniowanie własnej.</li> </ul> </li> </ul>	W	1



SEOD 138	<p>Praca z projektami aktów</p> <p>System musi umożliwiać:</p> <ul style="list-style-type: none"><li>A) Tworzenie aktu na podstawie innego aktu,</li><li>B) Kopiowanie wybranych jednostek lub grup jednostek pomiędzy aktami,</li><li>C) Blokowanie aktu,</li><li>D) Elektroniczne podpisywanie aktu (wbudowane biblioteki do podpisu obsługujące podpisy wydane przez dowolne, polskie centrum certyfikacji),</li><li>E) Elektroniczna kontrasygnata (podpis z wyłączeniem daty i numeru aktu),</li><li>F) Eksport aktu do: PDF, DOC, RTF, EDAP MSWiA,</li><li>G) Import uchwał budżetowych z programu BESTI@ oraz Wizja,</li><li>H) Import tabel z arkusza kalkulacyjnego Microsoft EXCEL oraz OpenOffice.org Calc</li><li>I) Automatyczne nadawanie ID dokumentu XML (identyczność wersji „papierowej” i elektronicznej).</li></ul>	W	1
SEOD 139	<p>W ramach tworzenie aktu zmieniającego w trybie standardowym (w powiązaniu z Bazą Aktów Własnych – BAW) system musi umożliwiać:</p> <ul style="list-style-type: none"><li>A) wyszukanie w BAW aktu, dla którego chcemy utworzyć akt zmieniający (jeżeli wskazany akt miał już zmiany, automatyczne wygenerowanie tekstu ujednoliconego dla tego aktu, który będzie zmieniany),</li><li>B) utworzenie nowego projektu aktu (z poziomu projektu aktu dostęp do treści i struktury aktu ujednoliconego),</li><li>C) zmiana aktu przy pomocy znaczników nowelizacyjnych: „zmień”, „dodaj”, „uchyl”,</li><li>D) automatycznie tworzenie treści aktu zmieniającego – wybór jednostki redakcyjnej ze struktury ujednoliconego aktu oraz użycie wybranego znacznika nowelizacyjnego tworzy treść aktu zmieniającego,</li><li>E) dostęp do treści ujednoliconej i porównawczej aktu prawnego generowanej ad-hoc i uwzględniającej wprowadzane zmiany</li></ul>	W	1
SEOD 140	<p>W ramach tworzenie aktu prawnego w trybie śledzenia zmian (w powiązaniu z Bazą Aktów Własnych – BAW) system musi umożliwiać:</p> <ul style="list-style-type: none"><li>A) wyszukanie w BAW aktu, dla którego chcemy utworzyć akt zmieniający (jeżeli wskazany akt miał już zmiany, automatyczne wygenerowanie tekstu ujednoliconego dla tego aktu, który będzie zmieniany),</li><li>B) utworzenie nowego projektu aktu i wczytanie treści ujednoliconej aktu w trybie edycji,</li><li>C) wprowadzanie zmian bezpośrednio w treści ujednoliconej aktu prawnego (w trybie śledzenia</li></ul>	W	1

	<p>zmian)</p> <p>D) wygenerowanie aktu zmieniającego na podstawie zmian wprowadzonych do tekstu ujednoliconego</p> <p>E) dostęp do treści ujednoliconej i porównawczej aktu prawnego generowanej ad-hoc i uwzględniającej wprowadzane zmiany.</p>		
SEOD 141	<p>System musi umożliwiać automatyczne generowanie obwieszczeń z tekstem jednolitym na podstawie aktu źródłowego i kolejnych zmian opublikowanych w Bazie Aktów Własnych, przy użyciu wbudowanego kreatora:</p> <p>A) możliwość wybrania jednostek redakcyjnych, które mają zostać pominięte w tekście jednolitym (jednostki wybierane z widoku drzewa struktury aktu źródłowego i kolejnych aktów zmieniających), w treści obwieszczenia:</p> <ul style="list-style-type: none"> <li>i automatycznie dodanie informacji o aktach zmieniających uwzględnionych przy tworzeniu obwieszczenia, wraz z przytoczeniem ich pełnych tytułów,</li> <li>ii automatycznie dodanie informacji o pominiętych jednostkach redakcyjnych wraz z przytoczeniem ich treści i tytułu aktu zmieniającego,</li> </ul> <p>B) w treści tekstu jednolitego stanowiącego załącznik do obwieszczenia:</p> <ul style="list-style-type: none"> <li>i automatyczne wygenerowanie przypisów nowelizacyjnych dla każdej zmiany wraz z podaniem pełnego tytułu aktu zmieniającego,</li> <li>ii automatyczne wygenerowanie przypisów dla jednostek pominiętych wraz z odwołaniem do odpowiedniego punktu w treści obwieszczenia,</li> </ul> <p>C) możliwość dowolnej ingerencji w treść wygenerowanego obwieszczenia</p>	W	1
SEOD 142	System musi umożliwiać tworzenia aktów zmieniających do tekstu jednolitego ogłoszonego obwieszczeniem i na tej podstawie tworzenia kolejnego obwieszczenia.	W	1
SEOD 143	<p>System musi umożliwiać określenia logiki tworzenia dokumentów zmieniających w przypadku:</p> <p>A) zmiany całego aktu (system automatycznie wstawia treść punktów zawierających zmiany, odnosząc się do zmienianego aktu),</p> <p>B) zmiany wskazanego załącznika –zmiany regulaminu /statutu, który stanowi załącznik do zarządzenia. (system automatycznie wstawia treść punktów zawierających zmiany, odnoszące się do zmienianego</p>	W	1



	załącznika).		
SEOD 144	<p>W ramach obsługi „rozstrzygnięć nadzorczych” – System musi umożliwiać uwzględnienia ewentualnego rozstrzygnięcia nadzorczego w tekście ujednoliconym aktu:</p> <ul style="list-style-type: none"><li>A) dla aktów nie posiadających aktów zmieniających automatyczne wygenerowanie tekstu ujednoliconego z informacją o rozstrzygnięciu),</li><li>B) dla aktów zmieniających (uwzględnienie treści rozstrzygnięcia w tekście ujednoliconym aktu, w przypadku gdy dla aktu zmieniającego wydano rozstrzygnięcie nadzorcze).</li></ul>	W	1
SEOD 145	<p>W ramach dedykowanej Bazy Aktów Własnych System musi umożliwiać udostępniającą funkcjonalności:</p> <ul style="list-style-type: none"><li>A) Możliwość prowadzenia:<ul style="list-style-type: none"><li>i zbioru aktów prawa miejscowego</li><li>ii zbioru uchwał rady, zarządu, zarządzeń wójta, burmistrza, itp.</li><li>iii dowolnych innych zbiorów – np. interpelacji radnych, rozstrzygnięć nadzorczych itd.</li></ul></li><li>B) Akty publikowane w zbiorach prowadzonych przez organy kadencyjne wyświetlane są w widoku kadencji z podziałem na poszczególne sesje.</li><li>C) Powiązania pomiędzy aktami:<ul style="list-style-type: none"><li>i możliwość ręcznego tworzenia powiązań pomiędzy publikowanym w BAW aktami prawnymi,</li><li>ii automatycznie tworzenie powiązań pomiędzy aktami zmienianymi i zmieniającymi utworzonymi przy użyciu Edytor XML, oraz pomiędzy aktem źródłowym a obwieszczeniem z tekstem jednolitym,</li><li>iii automatyczne generowanie tekstów ujednoliconych na każdą ewentualną zmianę dla aktów utworzonych przy użyciu Edytor XML,</li></ul></li><li>D) Wyszukiwanie aktów:<ul style="list-style-type: none"><li>i proste – przeszukiwanie po metadanych opublikowanych aktów na podstawie tekstu wpisanego w wyszukiwarkę</li><li>ii zaawansowane – możliwość określenia co najmniej typu aktu, zbioru aktów, hasła skrowidza, dat obowiązywania, tytułu,</li><li>iii pełnotekstowe w treści aktów, dodatkowo możliwość zawężenia wyszukiwania pełnotekstowego do zakresu określonego w wyszukiwaniu zaawansowanym,</li></ul></li><li>E) Zaawansowany skrowidz aktów:<ul style="list-style-type: none"><li>i predefiniowany wielopoziomowy skrowidz aktów prawnych zawierający zarówno hasła</li></ul></li></ul>	W	1



	<p>merytoryczne jak i hasła odsyłaczowe z powiązaniem do haseł merytorycznych,</p> <p>ii możliwość dodawania modyfikacji haseł skorowidza</p> <p>F) Rozbudowana, pełna metryka aktu zawierająca informacje o:</p> <p>i podstawowych metadanych aktu (typ aktu, organ wydający, numer, data, tytuł)</p> <p>ii aktach powiązanych,</p> <p>iii tekstach ujednoliconych,</p> <p>iv tekstach historycznych,</p> <p>v tekście aktu pierwotnego,</p> <p>vi aktów podobnych (wg przypisanych haseł skorowidza).</p> <p>G) Pełna obsługa dokumentów strukturalnych XML:</p> <p>i uzupełnianie metadanych aktów w momencie publikacji w BAW na podstawie danych z pliku XML aktu,</p> <p>ii możliwość przeglądania w HTML aktów publikowanych w formacie XML,</p> <p>H) Możliwość publikacji aktów w innych, dowolnych formatach, np.: PDF, HTML, DOC itp,</p> <p>I) Integracja z wojewódzkimi dziennikami urzędowymi, w zakresie pozwalającym na automatyczne dodanie do BAW informacji o publikacji aktu w dzienniku urzędowym i zmianie jego statusu na podstawie informacji o wejściu w życie danego aktu,</p> <p>J) Spełnienie wymogów dla BIP.</p> <p>i podstawowe wymagania W3C w zakresie zgodności ze standardem XHTML,</p> <p>ii posiada wersję dla osób słabo widzących (wysoki kontrast, powiększanie rozmiaru czcionki),</p> <p>iii pozwala na wyświetlanie treści z dostosowaniem do rozdzielczości ekranu użytkownika,</p> <p>iv zawiera dziennik zmian treści.</p> <p>K) Publikacja aktów i zarządzanie aplikacją:</p> <p>i publikacja i zarządzanie aktami możliwe z poziomu Edytor XML:</p> <ul style="list-style-type: none"><li>• przy publikacji możliwość utworzenia powiązania z aktem opublikowanym w dzienniku urzędowym (podając jedynie rok i pozycję aktu, automatycznie wygenerowanie linka do aktu w dzienniku),</li><li>• możliwość oznaczenia aktu jako „podlega publikacji w dzienniku” – w takim przypadku system automatycznie określi datę i adres publikacyjny aktu po</li></ul>		
--	---	--	--

	<p>opublikowaniu aktu w dzienniku urzędowym,</p> <ul style="list-style-type: none"> <li>• możliwość określenia dat obowiązywania aktu (data wejścia w życie, data utraty mocy, moc wsteczna), przy czym w przypadku oznaczenia aktu jako „podlega publikacji w dzienniku” data wejścia w życie określana automatycznie na podstawie reguły wejścia w życie (ilość dni od dnia publikacji w dzienniku)</li> </ul> <p>ii przypisanie aktu do zbioru i hasła (lub haseł) skorowidza,</p> <p>iii dla aktów nie utworzonych w Edytor XML możliwość dodania powiązań do aktów w BAW:</p> <ul style="list-style-type: none"> <li>• zmienia,</li> <li>• uchyla,</li> <li>• wykonuje,</li> <li>• unieważnia,</li> <li>• interpretuje,</li> <li>• jest rozstrzygnięciem nadzorczym dla,</li> <li>• jest orzeczeniem dla,</li> <li>• jest komentarzem,</li> <li>• jest tekstem jednolitym,</li> </ul> <p>iv dodanie relacji powoduje również dodanie relacji odwrotnej dla aktu opublikowanego w BAW,</p> <p>v dla aktów utworzonych w Edytor XML relacje dodawane automatycznie,</p> <p>vi konfiguracja aplikacji pozwala na:</p> <ul style="list-style-type: none"> <li>• dodawanie / usuwanie zbiorów aktów oraz zbiorów projektów aktów,</li> <li>• zmianę danych nagłówka portalu BAW, danych adresowych urzędu, loga,</li> <li>• edycję haseł skorowidza,</li> <li>• edycję organów wydających akty prawne,</li> <li>• definiowanie kadencji oraz sesji dla poszczególnych organów.</li> </ul>		
--	---	--	--

## 9.2 Wymagania pozafunkcjonalne w zakresie SEOD

	Wymagania pozafunkcjonalne w zakresie SEOD		
Wymaga- nie	Wymagania pozafunkcjonalne dotyczące Systemu Elektronicznego Obiegu Dokumentów	Funkcjonal- ność	Waga
	Architektura systemu		

SEODWP 1	System musi umożliwiać korzystanie z usług niezależnie od lokalizacji, z różnych rodzajów urządzeń., dla wskazanych użytkowników, w zależności od polityki bezpieczeństwa danego Partnera.	D	2
SEODWP 2	SEOD musi posiadać architekturę trójwarstwową.	W	1
SEODWP 3	System musi być w pełni transakcyjny i musi zabezpieczać dane przed zniszczeniem lub przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.	W	1
SEODWP 4	System od strony technicznej musi zapewnić skalowalność w zakresie wydajności, pojemności oraz dołączania dodatkowych użytkowników i elementów infrastruktury sprzętowej.	W	1
SEODWP 5	System musi zapewnić możliwość rozbudowy warstw poprzez zwiększenie zasobów komputerów obsługujących warstwę poprzez rozbudowę pamięci, zwiększenie liczby procesorów, zwiększanie liczby maszyn oraz zwiększenie pojemności pamięci masowych.	W	1
SEODWP 6	System musi być interoperacyjny w warstwie aplikacyjnej i bazodanowej – będzie pozwalał na uruchomienie w środowiskach systemowych bazujących na technologii Microsoft Windows oraz w środowiskach opartych na systemie Linux.	W	1
SEODWP 7	System musi umożliwiać rozpraszanie repozytorium dokumentów w ramach jednego systemu elektronicznego obiegu dokumentów na wiele komputerów rozmieszczonych w różnych lokalizacjach geograficznych (np. budynki urzędu).	O	3
	<b>Interfejs użytkownika</b>		
SEODWP 8	SEOD musi być systemem interoperacyjnym co najmniej w zakresie prezentacji danych: umożliwi uruchomienie systemu przez użytkownika końcowego z poziomu przeglądarki internetowej, co najmniej Internet Explorer, Firefox, Google Chrome, Opera w najnowszych wersjach. System musi być w pełni dostępny dla użytkownika pracującego na systemach operacyjnych z rodziny Windows (XP SP3/Vista/7/8), Linux (Ubuntu od wersji 12.04, Debian od wersji 6.0.5, Mint od wersji 11, Fedora od wersji 16, OpenSUSE od wersji 12.1), MacOS. System będzie działał w środowisku 32- i 64-bitowym.	D	1
SEODWP 9	SEOD musi cechować się interfejsem użytkownika opartym na intranetowych nowoczesnych rozwiązaniach: wykorzystywać menu, listy, formularze, przyciski, referencje (linki), itp.	W	1
SEODWP 10	Wymaga się, aby interfejs użytkownika SEOD stosował oznaczanie pól wymaganych na formularzu ekranowym w sposób wyróżniający te pola.	W	1

SEODWP 11	Organizacja pracy w ramach interfejsu użytkownika SEOD musi się opierać na zestawieniach podstawowych, prezentujących informacje znajdujące się w Systemie w formie syntetycznej (jako podsumowania, listy, zestawienia, grupy opcji, itp.) oraz na zestawieniach szczegółowych, tworzonych przez System w sytuacji, gdy zachodzi potrzeba zaprezentowania wskazanej przez użytkownika jednostki danych, np. konkretnego dokumentu elektronicznego, słownika parametrów systemowych, itp.	W	1
SEODWP 12	Interfejs użytkownika SEOD musi posiadać widok indywidualny, w ramach którego prezentowane będą tylko te składniki zawartości informacyjnej Systemu, za które odpowiedzialny jest węzeł struktury organizacyjnej, do którego przypisany jest dany użytkownik.	W	1
SEODWP 13	Wymaga się, aby widok indywidualny zawierał odnośniki do zestawień udostępniających wszystkie zadania realizowane przez pracowników danego węzła struktury organizacyjnej, dla których to zadań: A) termin zakończenia realizacji zadania już minął, B) termin zakończenia realizacji zadania mija za określoną w konfiguracji systemowej liczbę dni kalendarzowych.	W	1
SEODWP 14	Wymaga się, aby interfejs użytkownika zawierał informację o węźle struktury organizacyjnej, w którym aktualnie pracuje użytkownik.	W	1
SEODWP 15	Wymaga się, aby była możliwość konfiguracji widoków indywidualnych np. wysokość wiersza listy zawierającej sprawy, dokumenty, zadania(najmniejsza, mała, średnia, największa).	D	5
SEODWP 16	Wymaga się, aby była możliwość grupowania elementów (mechanizm drag&drop) na listach pism, spraw, zadań poprzez mechanizmy list przestawnych (grupowania zagnieżdżonego co najmniej do 20 poziomów). System musi umożliwiać zapamiętywanie zdefiniowanych grup dla konkretnego użytkownika.	D	1
SEODWP 17	Wymaga się, aby była możliwość przechodzenia z własnych list dokumentów i spraw na listy wskazanych osób., do których podglądu dany użytkownik jest uprawniony.	D	6
SEODWP 18	Wymaga się, aby była możliwość dowolnego ustawiania kolumn oraz zapamiętywania tych ustawień.	W	1
SEODWP 19	Wymaga się, aby była możliwość wyświetlania bądź ukrywania kolumn na listach spraw, dokumentów, zadań.	W	1
SEODWP 20	Wymaga się, aby była możliwość wykorzystania na listach spraw, dokumentów, zadań mechanizmów szybkiej filtracji po dowolnie wybranej kolumnie.	W	1
<b>Interfejsy integracyjne</b>			





SEODWP 21	System musi posiadać ustandaryzowane interfejsy zewnętrzne, obejmujące udostępnianie usług integracyjnych (m.in. wymiany danych) Systemu Elektronicznego Obiegu Dokumentów systemom zewnętrznym poprzez: usługi Web Services (w oparciu o standardy SOAP 1.2, WSDL co najmniej 1.1); możliwość komunikacji z wykorzystaniem plików XML zlokalizowanych w strukturach plikowych Partnera, zgodność ze standardami XML 1.0 i XSD 1.1 lub.; usługi JMS.	D	5
SEODWP 22	System musi umożliwiać administratorom tworzenie nowych oraz zarządzanie udostępnianymi usługami i interfejsami (w tym harmonogramem komunikacji, lokalizacją plików, uprawnieniami do nich) poprzez przyjazny interfejs. System będzie umożliwiał wdrażanie nowych interfejsów poprzez import konfiguracji, określającej standardy komunikacji z danym systemem, oraz serię kroków wykonywanych poprzez graficzny interfejs.	D	4
SEODWP 23	Dla danych pozyskiwanych z systemu zewnętrznego System musi umożliwiać administratorowi skonfigurowanie transformat oraz automatycznego przesyłania uzyskanych danych jako jednego lub wielu dokumentów do użytkownika lub użytkowników SEOD	D	1
	<b>Bezpieczeństwo, skalowalność i wydajność</b>		
SEODWP 24	System musi posiadać mechanizm kontroli dostępu do usług pozwalający na dostęp do danej usługi ze względu na użytkownika oraz grupę (jednostkę organizacyjną) do której należy.	W	1
SEODWP 25	System musi rejestrować wszystkie czynności dostępu do usług i zasobów w systemie, w zakresie dostępu przez użytkowników oraz aplikacje współpracujące z SEOD.	W	1
SEODWP 26	Oszacowanie wydajności musi uwzględniać okresowe (w określonych dniach roku) spiętrzenia prac skutkujące trzykrotnym wzrostem obciążenia w stosunku do obciążenia przeciętnego.	W	1
SEODWP 27	Odpowiednia pojemność systemu oznacza możliwość przechowywania w systemie takiej ilości danych, jaka średnio gromadzona jest w urzędzie o danej wielkości w okresie pięciu lat oraz dodatkowo 20% tej wielkości (zapas). Należy uwzględnić, że w systemie będą przechowywane pliki zawierające zeskanowane pisma wchodzące w postaci papierowej.	W	1
SEODWP 28	Jeżeli System dostarczony przez Wykonawcę nie będzie spełniał ww. wymagań lub przestanie je spełniać do 5 lat po dokonania odbioru końcowego, Wykonawca obowiązany jest odpowiednio uzupełnić sprzęt i oprogramowanie (np. poprzez zwiększenie pojemności dysków, mocy obliczeniowej, dostarczenie dodatkowych maszyn, licencji) bez dodatkowych kosztów po stronie Zamawiającego.	W	1

	<b>Zarządzalność systemu</b>		
SEODWP 29	SEOD musi umożliwić dystrybucję aktualizacji i monitorowanie wersji SEOD oraz oprogramowania pomocniczego z poziomu podsystemu centralnego zarządzania SeUI.	D	7
SEODWP 30	SEOD musi umożliwić monitorowanie wersji i konfiguracji oraz dystrybucję aktualizacji konfiguracji interfejsów integracyjnych SEOD z poziomu podsystemu centralnego zarządzania SeUI (przy czym część wdrożenia wykonywać może lokalny administrator przez interfejs graficzny).	D	6
SEODWP 31	SEOD musi zapewnić współpracę z systemem uprawnień SeUI (poprzez możliwość nadawania użytkownikom SEOD uprawnień w zakresie korzystania z aplikacji SeUI) i umożliwić Single Sign-On w obrębie systemu PseAP.	D	3
	<b>Wymagania prawne</b>		
SEODWP 32	SEOD musi być zgodny z przepisami prawa, obowiązującymi na dzień ostatecznego odbioru systemu oraz opublikowanymi aktami prawnymi z określoną datą wejścia w życie (nawet, jeżeli ta data jest po dniu ostatecznego odbioru systemu).	W	1
	<b>Inne wymagania</b>		
SEODWP 33	System musi umożliwić obsługę plików (dokumentów) w dowolnym formacie zgodnym z obowiązującymi przepisami prawa (pliki te są otwierane i modyfikowane przez użytkowników w odrębnych aplikacjach, jednak mogą być przedmiotem obiegu w EOD).	W	1
SEODWP 34	System musi posiadać wbudowany mechanizm zdalnej asysty technicznej pozwalający na wsparcie użytkowników systemu przez uprawnionych do tego administratorów	D	8

### 9.3 Wdrożenie SEOD

Na 30 dni przed przystąpieniem do wdrożenia produkcyjnego Wykonawca musi dostarczyć Plan Wdrożenia SEOD. Plan Wdrożenia SEOD zostanie przyjęty w wyniku obopólnych ustaleń między Wykonawcą a Zamawiającym. Integralną częścią Planu Wdrożenia SEOD powinny być:

- Opis zadań, procedur i obowiązków stron oraz harmonogram Wdrożenia Pilotażowego;
- Opis zadań, procedur i obowiązków stron oraz harmonogram Wdrożenia Produkcyjnego;

W szczególności opisane zostaną procedury odbiorów:

- Dokumentacji;
- Testów;
- Instruktaży stanowiskowych;
- Systemu u poszczególnych typów Partnerów;
- Procedura Odbioru Końcowego.

### 9.3.1 Wdrożenie produkcyjne systemu

Wymaganie	Minimalne wymagania dotyczące Etapu wdrożenia produkcyjnego Systemu
	<b>Zasady ogólne</b>
SWPRS 1	Wdrożenie produkcji Systemu musi obejmować sekwencję wdrożeń produkcyjnych w poszczególnych JST.
SWPRS 2	Warunkiem odbioru wdrożenia produkcyjnego SEOD jest przeprowadzenie z pozytywnym wynikiem kompletu testów funkcjonalnych i pozafunkcjonalnych SEOD. Testy pozafunkcjonalne powinny zostać przeprowadzone na jednej lub więcej instancjach Systemu (dla testów, których przeprowadzenie na różnych platformach sprzętowych, pod różnym obciążeniem oraz w różnych konfiguracjach jest zasadne).
SWPRS 3	Oprócz testów pozafunkcjonalnych zostaną przeprowadzone dodatkowo testy stabilności Systemu u tych Partnerów, u których było wcześniej prowadzone wdrożenie pilotażowe. Testy stabilności będą prowadzone na takich zasadach jak dla SeUI (zob. rozdział 8.5), po przekazaniu SEOD u tych Partnerów do eksploatacji, a ich pozytywne zakończenie będzie warunkowało końcowy odbiór wdrożenia produkcyjnego SEOD.
SWPRS 4	Wykonawca jest zobowiązany do uzyskania protokołów odbioru wdrożenia produkcyjnego (tzw. protokoły cząstkowe) od wszystkich JST objętych wdrożeniem Systemu, co będzie – wraz z protokołami z testów funkcjonalnych, pozafunkcjonalnych i stabilności – równoznaczne z potwierdzeniem odbioru wdrożenia produkcyjnego Systemu przez Zamawiającego.
	<b>Instalacja, uruchomienie i parametryzacja Systemu</b>
SWPRS 5	Wykonawca odpowiada za dostawę licencji oraz zainstalowanie niezbędnego do zgodnej z OPZ pracy Systemu oprogramowania na przeznaczonych do tego celu zestawach serwerowych.
SWPRS 6	Wykonawca odpowiada za uruchomienie zainstalowanego oprogramowania, tym samym: <ul style="list-style-type: none"> <li>A) Wykonawca musi przeprowadzić rozruch zainstalowanego oprogramowania.</li> <li>B) Wykonawca odpowiada za wprowadzenie do Systemu danych konfiguracyjnych niezbędnych do poprawnej zgodnej z OPZ pracy SEOD.</li> <li>C) Parametryzacja SEOD obejmuje wprowadzenie ustawień umożliwiających współpracę Systemu, zgodną z dostarczoną dokumentacją i instrukcjami</li> </ul>

	<p>użytkownika, z istniejącym w JST środowiskiem sprzętowym oraz oprogramowaniem, w skład którego wchodzi co najmniej:</p> <ul style="list-style-type: none"> <li>i urządzenia peryferyjne wykorzystywane przez użytkowników Systemu;</li> <li>ii urządzenia sieciowe LAN oraz WAN zapewniające komunikację pomiędzy użytkownikami a Systemem;</li> <li>iii wchodzące w skład zestawu serwerowego rozwiązanie do tworzenia kopii zapasowych;</li> <li>iv oprogramowanie podstawowe i pomocnicze SEOD;</li> </ul> <p>D) Parametryzacja SEOD obejmuje wprowadzenie ustawień umożliwiających właściwą współpracę Systemu z innymi systemami informatycznymi, w tym co najmniej:</p> <ul style="list-style-type: none"> <li>i skonfigurowanie połączenia z systemem e-usług internetowych, zapewniającego współpracę obu systemów zgodnie z założeniami projektu.</li> </ul> <p>E) W zakres parametryzacji SEOD wchodzi wprowadzenie danych opisujących indywidualną specyfikę JST w zakresie:</p> <ul style="list-style-type: none"> <li>i zdefiniowanie struktury organizacyjnej JST;</li> <li>ii zdefiniowanie JRWA JST</li> <li>iii inicjalizacja odpowiednich rejestrów;</li> <li>iv utworzenie kont użytkowników SEOD oraz wprowadzenie danych o użytkownikach Systemu;</li> <li>v powiązanie użytkowników Systemu z węzłami struktury organizacyjnej;</li> <li>vi wprowadzenie innych ustawień sterujących zachowaniem Systemu, zgodnie z preferencjami określonymi przez JST na etapie zbierania danych konfiguracyjnych</li> <li>vii wdrożenie pięciu ścieżek elektronicznego obiegu dokumentów dla każdego z Partnerów.</li> </ul> <p>F) W zakresie organizacji procesu zbierania danych konfiguracyjnych, dopuszcza się zastosowanie przez Wykonawcę kwestionariuszy elektronicznych posiadających funkcje automatycznej walidacji wprowadzanych danych. Jednak Wykonawca musi dopuścić możliwość przekazania danych w takiej formie elektronicznej, jaką dany Partner już posiada.</p> <p>G) Wykonawca wspólnie z Zamawiającym powinien przeprowadzić weryfikację otrzymanych od Zamawiającego danych konfiguracyjnych</p>
--	--

	pod kątem ich poprawności formalnej oraz spójności logicznej. Jeżeli niezgodne z oczekiwaniami Zamawiającego działanie Systemu zostało spowodowane wprowadzeniem niezweryfikowanych danych konfiguracyjnych, jest ono traktowane jak błąd uniemożliwiający odbiór wdrożenia Systemu przez Zamawiającego.
--	--

### 9.3.2 Formalne przekazanie SEOD do eksploatacji

Wymaganie	Minimalne wymagania dotyczące Formalnego przekazania SEOD do eksploatacji u Beneficjenta
	<b>Ogólne</b>
PDE 1	Odbiór wdrożenia produkcyjnego Systemu przez zamawiającego stanowi warunek, który musi zostać obligatoryjnie spełniony, aby Zamawiający mógł następnie dokonać formalnego przekazania SEOD do eksploatacji.
PDE 2	W terminie przekazania systemu do eksploatacji u danego Partnera Wykonawca zobowiązany będzie do zapewnienia ciągłego wsparcia eksperckiego na miejscu instalacji Systemu. Minimalny wymiar tej usługi zależy od całkowitej liczby użytkowników SEOD w organizacji Partnera i określany jest w sposób następujący: <ul style="list-style-type: none"> <li>A) Od 1 do 50 użytkowników SEOD – 1 dzień roboczy 1 specjalisty.</li> <li>B) Od 51 do 150 użytkowników SEOD – 2 dni robocze 1 specjalisty.</li> <li>C) Powyżej 150 użytkowników SEOD – 3 dni robocze 1 specjalisty</li> <li>D) Powyżej 200 użytkowników SEOD - 5 dni roboczych 1 specjalisty.</li> </ul>
PDE 3	W zakres odpowiedzialności specjalistów Wykonawcy wchodzi zestaw zadań, które obejmują co najmniej: <ul style="list-style-type: none"> <li>A) Śledzenie pracy SEOD i rozwiązywanie bieżących problemów zagrażających stabilnemu działaniu Systemu.</li> <li>B) Weryfikacja i ewentualne dostosowanie parametrów konfiguracyjnych Systemu do specyfiki Beneficjenta.</li> <li>C) Dokonanie odpowiednich czynności w SEUI – włączenie SEOD i jego użytkowników w System PSeAP.</li> <li>D) Wytworzenie sprawozdania z formalnego przekazania SEOD do eksploatacji.</li> </ul>

## 10 Oprogramowanie standardowe

Przedmiotem zamówienia jest zakup oprogramowania wraz z bezterminowymi licencjami oraz subskrypcji oprogramowania. Liczba licencji musi być wystarczająca dla podanej liczby komputerów oraz użytkowników, zgodnie z zasadami licencjonowania stosowanymi przez podmiot posiadający autorskie prawa majątkowe do oprogramowania<sup>2</sup>. Liczby zapotrzebowanych pakietów biurowych typu I i II znajdują się w tabeli w Załączniku nr 1 do niniejszego OPZ.

Typ oprogramowania
Pakiet biurowy typ I
Pakiet biurowy typ II
System operacyjny dla komputerów PC
Serwerowy system operacyjny z elementami zarządzania
Licencje dostępowe do serwerowego systemu operacyjnego (na użytkownika)
Serwer portalu Internet
Serwer relacyjnej bazy danych

Wymagania ogólne w zakresie licencji standardowych:

- Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej licencje pochodzące od jednego producenta, umożliwiające wykorzystanie wspólnych i jednolitych procedur uaktualniania, zarządzania i monitorowania.
- Licencjonowanie musi uwzględniać (w okresie przynajmniej 5 lat od dnia dokonania odbioru końcowego) prawo do bezpłatnej instalacji udostępnianych przez producenta oprogramowania uaktualnień i poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania, z wyłączeniem licencji podlegających subskrypcji. W przypadku subskrypcji (np. oprogramowanie antywirusowe) wymagania odnośnie okresu subskrypcji będą podawane przy opisie danego oprogramowania.

Wymagania w zakresie licencji (z wyłączeniem systemu operacyjnego dla komputerów PC).

- Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi i serwerami (np. w przypadku wymiany sprzętu) oraz możliwość sublicencjonowania dla jednostek stowarzyszonych.
- Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych (możliwość kopiowanie oprogramowania

---

<sup>2</sup> Na przykład w przypadku stosowania licencji na procesor serwera liczba licencji musi być równa liczbie procesorów w dostarczanych serwerach.

na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.

## 10.1 Pakiet biurowy typ I

Wymaganie	Minimalne wymagania dotyczące Pakietu biurowego typ I
PB I 1	<p><u>Wymagania odnośnie interfejsu użytkownika:</u></p> <ul style="list-style-type: none"> <li>A) Pełna polska wersja językowa interfejsu użytkownika</li> <li>B) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych</li> <li>C) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitorowania go o ponowne uwierzytelnienie się.</li> </ul>
PB I 2	<p>Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:</p> <ul style="list-style-type: none"> <li>A) posiada kompletny i publicznie dostępny opis formatu,</li> <li>B) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych(Dz.U.05.212.1766),</li> <li>C) umożliwia wykorzystanie schematów XML,</li> <li>D) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1. załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych(Dz.U.05.212.1766).</li> </ul>
PB I 3	Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
PB I 4	W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
PB I 5	Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
PB I 6	<p>Pakiet zintegrowanych aplikacji biurowych musi zawierać:</p> <ul style="list-style-type: none"> <li>A) Edytor tekstów.</li> </ul>

	<p>B) Arkusz kalkulacyjny.</p> <p>C) Narzędzie do przygotowywania i prowadzenia prezentacji.</p> <p>D) Narzędzie do tworzenia drukowanych materiałów informacyjnych.</p> <p>E) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).</p>
PB I 7	<p>Edytor tekstów musi umożliwiać:</p> <p>A) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.</p> <p>B) Wstawianie oraz formatowanie tabel.</p> <p>C) Wstawianie oraz formatowanie obiektów graficznych.</p> <p>D) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).</p> <p>E) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.</p> <p>F) Automatyczne tworzenie spisów treści.</p> <p>G) Formatowanie nagłówków i stopek stron.</p> <p>H) Sprawdzanie pisowni w języku polskim.</p> <p>I) Śledzenie zmian wprowadzonych przez użytkowników.</p> <p>J) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.</p> <p>K) Określenie układu strony (pionowa/pozioma).</p> <p>L) Wydruk dokumentów.</p> <p>M) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.</p> <p>N) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.</p> <p>O) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.</p> <p>P) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym</p>



	<p>prawem.</p> <p>Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującymi w Polsce prawa.</p> <p>Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.</p>
PB I 8	<p><u>Arkusze kalkulacyjne</u> musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Tworzenie raportów tabelarycznych.</li> <li>B) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.</li> <li>C) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.</li> <li>D) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).</li> <li>E) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.</li> <li>F) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.</li> <li>G) Wyszukiwanie i zamianę danych.</li> <li>H) Wykonywanie analiz danych przy użyciu formatowania warunkowego.</li> <li>I) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.</li> <li>J) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.</li> <li>K) Formatowanie czasu, daty i wartości finansowych z polskim formatem.</li> <li>L) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.</li> <li>M) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.</li> </ul>

	N) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
PB I 9	<p><u>Narzędzie do przygotowywania i prowadzenia prezentacji</u> musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Przygotowywanie prezentacji multimedialnych, które będą: <ul style="list-style-type: none"> <li>i Prezentowanie przy użyciu projektora multimedialnego</li> <li>ii Drukowanie w formacie umożliwiającym robienie notatek</li> <li>iii Zapisanie jako prezentacja tylko do odczytu.</li> </ul> </li> <li>B) Nagrywanie narracji i dołączanie jej do prezentacji</li> <li>C) Opatrywanie slajdów notatkami dla prezentera</li> <li>D) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo</li> <li>E) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego</li> <li>F) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym</li> <li>G) Możliwość tworzenia animacji obiektów i całych slajdów</li> <li>H) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera</li> <li>I) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.</li> </ul>
PB I 10	<p><u>Narzędzie do tworzenia drukowanych materiałów informacyjnych</u> musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Tworzenie i edycję drukowanych materiałów informacyjnych.</li> <li>B) Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.</li> <li>C) Edycję poszczególnych stron materiałów.</li> <li>D) Podział treści na kolumny.</li> <li>E) Umieszczanie elementów graficznych.</li> <li>F) wykorzystanie mechanizmu korespondencji seryjnej.</li> <li>G) Płynne przesuwanie elementów po całej stronie publikacji.</li> <li>H) Eksport publikacji do formatu PDF oraz TIFF.</li> <li>I) Wydruk publikacji.</li> <li>J) Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.</li> </ul>

PB I 11	<p><u>Narzędzie do zarządzania informacją prywatną</u> (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.</li> <li>B) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.</li> <li>C) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.</li> <li>D) Automatyczne grupowanie poczty o tym samym tytule.</li> <li>E) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.</li> <li>F) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia.</li> <li>G) Zarządzanie kalendarzem.</li> <li>H) Udostępnianie kalendarza innym użytkownikom.</li> <li>I) Przeglądanie kalendarza innych użytkowników.</li> <li>J) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.</li> <li>K) Zarządzanie listą zadań.</li> <li>L) Zlecanie zadań innym użytkownikom.</li> <li>M) Zarządzanie listą kontaktów.</li> <li>N) Udostępnianie listy kontaktów innym użytkownikom.</li> <li>O) Przeglądanie listy kontaktów innych użytkowników.</li> <li>P) Możliwość przysyłania kontaktów innym użytkownikom.</li> </ul>
PB I 12	<u>Pakiet musi pracować w środowisku dostarczanego systemu operacyjnego.</u>

## 10.2 Pakiet biurowy typ II

Wymaganie	Minimalne wymagania dotyczące Pakietu biurowego typ II
PB II 1	Pakiet biurowy typu II musi spełniać wszystkie wymagania Pakietu biurowego typu I a ponadto:
PB II 2	<p>Wymagania odnośnie interfejsu użytkownika:</p> <p>Pełna polska wersja językowa interfejsu użytkownika musi posiadać z możliwość przełączania wersji językowej interfejsu na język angielski</p>
PB II 3	<p>Pakiet zintegrowanych aplikacji biurowych musi dodatkowo zawierać:</p> <ul style="list-style-type: none"> <li>A) Narzędzie do tworzenia i pracy z lokalną bazą danych.</li> <li>B) Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu</li> </ul>

	wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
PB II 4	<p><u>Narzędzie do tworzenia i wypełniania formularzy elektronicznych</u> musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania.</li> <li>B) Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków.</li> <li>C) Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników.</li> <li>D) Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych.</li> <li>E) Możliwość pobierania danych z platformy do pracy grupowej.</li> <li>F) Przesłanie danych przy użyciu usługi Web (tzw. web service).</li> <li>G) Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML.</li> <li>H) Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.</li> </ul>
PB II 5	<p><u>Narzędzie do tworzenia i pracy z lokalną bazą danych</u> musi umożliwiać:</p> <ul style="list-style-type: none"> <li>A) Tworzenie bazy danych przez zdefiniowanie:</li> <li>B) Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.</li> <li>C) Relacji pomiędzy tabelami.</li> <li>D) Formularzy do wprowadzania i edycji danych.</li> <li>E) Raportów.</li> <li>F) Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych.</li> <li>G) Tworzenie bazy danych przy użyciu zdefiniowanych szablonów.</li> <li>H) Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.</li> </ul>
PB II 6	<p><u>Narzędzie komunikacji wielokanałowej</u> stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:</p> <ul style="list-style-type: none"> <li>A) Pełna polska wersja językowa interfejsu użytkownika.</li> </ul>

	<p>B) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.</p> <p>C) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.</p> <p>D) Możliwość obsługi tekstowych wiadomości błyskawicznych.</p> <p>E) Możliwość komunikacji głosowej i video.</p> <p>F) Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.</p> <p>G) Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.</p> <p>H) Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.</p>
PB II 7	<u>Pakiet musi pracować w środowisku dostarczanego systemu operacyjnego.</u>

### 10.3 System operacyjny dla komputerów PC

Wymaganie	Minimalne wymagania dotyczące Systemu operacyjnego dla komputerów PC
SO PC 1	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.
SO PC 2	Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek.
SO PC 3	Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu.
SO PC 4	Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW.
SO PC 5	Internetowa aktualizacja zapewniona w języku polskim.
SO PC 6	Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.

SO PC 7	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediiów, pomoc, komunikaty systemowe.
SO PC 8	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
SO PC 9	Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
SO PC 10	Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.
SO PC 11	Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
SO PC 12	Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
SO PC 13	Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
SO PC 14	Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.
SO PC 15	Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modulem „uczenia się” głosu użytkownika.
SO PC 16	Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
SO PC 17	Wbudowany system pomocy w języku polskim.
SO PC 18	Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
SO PC 19	Zarządzanie stacją roboczą poprzez polityki rozumiane jako zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
SO PC 20	Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach

	reguł definiujących ustawienia zarządzanych w sposób centralny.
SO PC 21	Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
SO PC 22	Wsparcie dla logowania przy pomocy smartcard.
SO PC 23	Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
SO PC 24	Posiadanie narzędzi służących do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
SO PC 25	Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
SO PC 26	Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
SO PC 27	Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
SO PC 28	Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
SO PC 29	Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
SO PC 30	Graficzne środowisko instalacji i konfiguracji.
SO PC 31	Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
SO PC 32	Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
SO PC 33	Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
SO PC 34	Możliwość przywracania plików systemowych.
SO PC 35	System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do

	kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
SO PC 36	System musi posiadać możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

#### 10.4 Serwerowy system operacyjny z elementami zarządzania

Wymaganie	Minimalne wymagania dotyczące Serwerowego systemu operacyjnego
SSO 1	Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.
SSO 2	Możliwość wykorzystania, co najmniej 8 fizycznych procesorów x64 oraz co najmniej 2 TB pamięci RAM.
SSO 3	Wsparcie (na umożliwiającym to sprzęcie) dodawania pamięci RAM bez przerywania pracy.
SSO 4	Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego
SSO 5	Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
SSO 6	Wbudowane wsparcie instalacji i pracy na wolumenach które: A) pozwalają na zmianę rozmiaru w czasie pracy systemu, B) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, C) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, D) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
SSO 7	Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
SSO 8	Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
SSO 9	Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.



SSO 10	Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
SSO 11	Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
SSO 12	Graficzny interfejs użytkownika.
SSO 13	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
SSO 14	Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
SSO 15	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
SSO 16	Obsługa platform sprzętowych x86, x64.
SSO 17	Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
SSO 18	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
SSO 19	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
SSO 20	<p>Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> <li>A) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.</li> <li>B) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: <ul style="list-style-type: none"> <li>i Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,</li> <li>ii Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,</li> <li>iii Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</li> </ul> </li> <li>C) Zdalna dystrybucja oprogramowania na stacje robocze.</li> </ul>

	<p>D) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</p> <p>E) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ul style="list-style-type: none"> <li>i Dystrybucję certyfikatów poprzez http,</li> <li>ii Konsolidację CA dla wielu lasów domeny,</li> <li>iii Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.</li> </ul> <p>F) Szyfrowanie plików i folderów.</p> <p>G) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>H) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</p> <p>I) Serwis udostępniania stron WWW.</p> <p>J) Wsparcie dla protokołu IP w wersji 6 (IPv6).</p> <p>K) Wbudowane usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.</p> <p>L) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na tworzenie do 4 maszyn wirtualnych ze zgodnym z platformą sprzętową systemem operacyjnym. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ul style="list-style-type: none"> <li>i Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych.</li> <li>ii Obsługa ramek typu jumbo frames dla maszyn wirtualnych.</li> </ul>
SSO 21	Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
SSO 22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
SSO 23	Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego
SSO 24	Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

SSO 25	Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
SSO 26	Zorganizowany system szkoleń i materiały edukacyjne w języku polskim, na przykład w postaci samouczka dostępnego z poziomu systemu.

#### 10.4.1 Zarządzanie środowiskami serwerowymi

Wzmaganie	Wymagania dotyczące zarządzania środowiskami serwerowymi
ZŚS	Elementy zarządzania środowiskami serwerowymi muszą spełniać niżej wymienione wymagania:
ZŚS 1	Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym.
ZŚS 2	Oprogramowanie musi być licencjonowane na zarządzanie dostarczoną architekturą. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji.
ZŚS 3	Licencja musi uprawniać do zarządzania dowolną liczbą środowisk systemu operacyjnego na tym serwerze.
ZŚS 4	Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach: <ul style="list-style-type: none"> <li>A) System zarządzania infrastrukturą i oprogramowaniem.</li> <li>B) System zarządzania komponentami.</li> <li>C) System zarządzania środowiskami wirtualnym.</li> <li>D) System tworzenia kopii zapasowych.</li> <li>E) System automatyzacji zarządzania środowisk IT.</li> <li>F) System zarządzania incydentami i problemami.</li> <li>G) Ochrona antymalware.</li> </ul>

#### 10.5 System zarządzania infrastrukturą i oprogramowaniem

Wymaganie	Wymagania dotyczące systemu zarządzania infrastrukturą i oprogramowaniem
SZliP 1 ZliP	System zarządzania infrastrukturą i oprogramowaniem musi niżej wymienione wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:
SZliP 2	<u>Inwentaryzacja i zarządzanie zasobami:</u> <ul style="list-style-type: none"> <li>A) Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania.</li> </ul>

	<p>B) Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu.</p> <p>C) Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp).</p> <p>D) System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta.</p> <p>E) Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera.</p>
SZiIP 3	<p><u>Użytkowane oprogramowanie – pomiar wykorzystania</u></p> <p>A) System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania.</p> <p>B) Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.</p>
SZiIP 4	System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.
SZiIP 5	<p><u>Definiowanie i sprawdzanie standardu serwera:</u></p> <p>A) System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej.</p> <p>B) Reguły powinny sprawdzać następujące elementy systemu komputerowego lub ich równoważne odpowiedniki:</p> <ul style="list-style-type: none"> <li>i stan usługi (Windows Service),</li> <li>ii obecność poprawek (Hotfix),</li> <li>iii WMI,</li> <li>iv rejestr systemowy,</li> <li>v system plików,</li> <li>vi Active Directory,</li> <li>vii SQL (query),</li> </ul>

	viii Metabase.
SZliP 6	<p><u>Raportowanie, prezentacja danych:</u></p> <p>A) System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub</p> <p>B) Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services.</p> <p>C) System powinien posiadać predefiniowane raport w następujących kategoriach:</p> <ul style="list-style-type: none"> <li>i Sprzęt (inventaryzacja).</li> <li>ii Oprogramowanie (inventaryzacja).</li> <li>iii Oprogramowanie (wykorzystanie).</li> <li>iv Oprogramowanie (aktualizacje, w tym system operacyjny).</li> </ul> <p>D) System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport.</p> <p>E) System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu.</p>
SZliP 7	<p><u>Analiza działania systemu, logi, komponenty</u></p> <p>A) Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy.</p> <p>B) Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.</p>

### 10.5.1 System zarządzania komponentami

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając poniższe wymagania.

Wymaganie	Wymagania dotyczące zarządzania komponentami
SZK 1	<p><u>Architektura</u></p> <p>A) Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.</p> <p>B) Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji</p>

	<p> pewnych grup komputerów/usług.</p> <p>C) System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.</p> <p>D) Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.</p> <p>E) Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.</p> <p>F) Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.</p> <p>G) Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).</p> <p>H) Wsparcie dla protokołu IPv6.</p> <p>I) System powinien udostępniać funkcje autodiagnostyczne, w tym:</p> <ul style="list-style-type: none"> <li>i. monitorowanie stanu klientów,</li> <li>ii. możliwość automatycznego lub administracyjnego restartu klienta,</li> <li>iii. możliwość reinstalacji klienta.</li> </ul>
SZK 2	<p><u>Audyt zdarzeń bezpieczeństwa</u></p> <p>System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:</p> <p>A) Przekazywanie zdarzeń z podległych klientów w czasie „prawie” rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).</p> <p>B) Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.</p> <p>C) Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst” – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.</p>
SZK 3	<p><u>Konfiguracja i monitorowanie</u></p> <p>System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:</p> <p>A) Monitorowane obiekty powinny być grupowane (klasy) w oparciu</p>

	<p>o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu.</p> <p>B) Powinny być wykrywane - co najmniej, atrybuty pobierane z:</p> <ul style="list-style-type: none"> <li>i rejestru,</li> <li>ii WMI,</li> <li>iii OLEDB,</li> <li>iv LDAP,</li> <li>v skrypty (uruchamiane w celu wykrycia atrybutów obiektu).</li> </ul> <p>W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.</p> <p>C) Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp.</p> <p>D) Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp. elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestaw monitorujące, co najmniej dla:</p> <ul style="list-style-type: none"> <li>i Windows Server 2003/2008/2008R2,</li> <li>ii Active Directory 2003/2008,</li> <li>iii Exchange 2003/2007/2010,</li> <li>iv Microsoft SharePoint 2003/2007/2010,</li> <li>v Microsoft SharePoint Services 3.0,</li> <li>vi Microsoft SharePoint Foundation 2010,</li> <li>vii SQL 2005/2008/2008R2 (x86/x64/ia64),</li> <li>viii Windows Client OS (XP/Vista/7),</li> <li>ix Information Worker (Office, IExplorer, Outlook, itp...),</li> <li>x IIS 6.0/7.0/7.5,</li> <li>xi HP-UX 11i v2/v3,</li> <li>xii Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86),</li> <li>xiii Red Hat Enterprise Linux 4/5/6 (x86/x64) Server,</li> <li>xiv Novell SUSE Linux Enterprise Server 9/10SP1/11,</li> <li>xv IBM AIX v5.3 i v6.1/v7.1 (POWER).</li> </ul>
--	---

	<p>E) System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.</p> <p>F) System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:</p> <ul style="list-style-type: none"> <li>i interfejsy sieciowe</li> <li>ii porty</li> <li>iii sieci wirtualne (VLAN)</li> <li>iv grupy Hot Standby Router Protocol (HSRP)</li> </ul> <p>G) System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:</p> <ul style="list-style-type: none"> <li>i SNMP (trap, probe),</li> <li>ii WMI Performance Counters,</li> <li>iii Log Files (text, text CSV),</li> <li>iv Windows Events (logi systemowe),</li> <li>v Windows Services,</li> <li>vi Windows Performance Counters (perflib),</li> <li>vii WMI Events,</li> <li>viii Scripts (wyniki skryptów, np.: WSH, JSH),</li> <li>ix Unix/Linux Service,</li> <li>x Unix/Linux Log.</li> </ul> <p>H) Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów.</p>
SZK 4	<p><u>Tworzenie reguł:</u></p> <p>A) W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:</p> <ul style="list-style-type: none"> <li>i Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event),</li> <li>ii Performance based (SNMP performance, WMI performance, Windows performance),</li> <li>iii Probe based (scripts: event, performance).</li> </ul> <p>B) System musi umożliwiać przekazywanie zebranych przez reguły</p>



	<p>informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.</p> <p>C) Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:</p> <ul style="list-style-type: none"> <li>i na ilość takich samych próbek o takiej samej wartości,</li> <li>ii na procentową zmianę od ostatniej wartości próbki.</li> </ul> <p>D) Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia” się monitorowanego parametru w zakresie przebiegu bazowego „baseline” w zadanym okresie czasu.</p> <p>E) System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.</p> <p>F) System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:</p> <ul style="list-style-type: none"> <li>i ASP .Net Application,</li> <li>ii ASP .Net Web Service,</li> <li>iii OLE DB,</li> <li>iv TCP Port,</li> <li>v Web Application,</li> <li>vi Windows Service,</li> <li>vii Unix/Linux Service,</li> <li>viii Process Monitoring.</li> </ul> <p>Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji.</p> <p>G) System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.</p> <p>H) Z każdym elementem monitorującym (monitor, reguła, alarm, itp...) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).</p> <p>I) System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych</p>
--	--

	<p>potem do celów analitycznych.</p> <p>J) System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostępność), i licznika wydajności (z agregacją dla wartości – min, max, avg).</p>
SZK 5	<p><u>Przechowywanie i dostęp do informacji</u></p> <p>A) Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp...) powinny być przechowywane w bazie danych operacyjnych.</p> <p>B) System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.</p> <p>C) System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).</p> <p>D) System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystane w celu rozszerzenia tej funkcjonalności.</p> <p>E) System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.</p> <p>F) System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:</p> <ul style="list-style-type: none"> <li>i XML,</li> <li>ii CSV,</li> <li>iii TIFF,</li> <li>iv PDF,</li> <li>v XLS,</li> <li>vi Web archive.</li> </ul>
SZK 6	<p><u>Konsola systemu zarządzania</u></p> <p>A) Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.</p> <p>B) System powinien udostępniać dwa rodzaje konsoli:</p> <ul style="list-style-type: none"> <li>i w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna),</li> <li>ii w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).</li> </ul> <p>C) Konsola zdalna powinna umożliwiać definiowanie każdemu</p>

	<p>użytkownikowi własnych widoków, co najmniej w kategoriach:</p> <ul style="list-style-type: none"> <li>i Alerts,</li> <li>ii Events,</li> <li>iii State,</li> <li>iv Performance,</li> <li>v Diagram,</li> <li>vi Task Status,</li> <li>vii Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).</li> </ul> <p>D) Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.</p> <p>E) Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdują (po typie, ważności, typach obiektów, itp.), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych”.</p> <p>F) Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.</p> <p>G) Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:</p> <ul style="list-style-type: none"> <li>i opcji definiowania ról użytkowników,</li> <li>ii opcji definiowania widoków,</li> <li>iii opcji definiowania i generowania raportów,</li> <li>iv opcji definiowania powiadomień,</li> <li>v opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących,</li> <li>vi opcji instalacji/deinstalacji klienta.</li> </ul> <p>H) Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).</p>
SZK 7	<p><u>Wymagania dodatkowe</u></p> <p>System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalającą m.in. na:</p> <ul style="list-style-type: none"> <li>A) Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo).</li> <li>B) Wykonywanie operacji w systemie z poziomu linii poleceń.</li> <li>C) Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania.</li> <li>D) Podłączenie do aplikacji biurowych pozwalające na integrację</li> </ul>

	statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie.
--	--

### 10.5.2 System automatyzacji zarządzania środowisk IT

Wymaganie	Wymagania dotyczące systemu automatyzacji zarządzania środowisk IT
SAZŚ IT 1	System automatyzacji zarządzania środowisk IT musi udostępniać bezkryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.
SAZŚ IT 2	System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.
SAZŚ IT 3	System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.
SAZŚ IT 4	System musi wspomagać planowanie i automatyzację wdrażania poprawek.
SAZŚ IT 5	System musi umożliwiać zarządzanie życiem środowisk wirtualnych.
SAZŚ IT 6	System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania workflow.
SAZŚ IT 7	System musi posiadać wbudowane (gotowe) workflow, takie jak: <ul style="list-style-type: none"> <li>A) Active Directory Password Reset</li> <li>B) Microsoft Cluster Patching</li> <li>C) Microsoft SQL Server Cluster Patching</li> <li>D) Microsoft SQL: Server Dump Copy Load</li> <li>E) Operations Manager Event Remediation</li> <li>F) Operations Manager Event Remediation and Enrichment</li> <li>G) Operations Manager Service Alert Testing</li> <li>H) VM Provisioning</li> <li>I) Working with FTP</li> <li>J) Operations Manager Tool Integration</li> <li>K) Operations Manager: Manager of Managers</li> <li>L) Operations Manager: Maintenance Windows</li> <li>M) Active Directory: New Employee Onboarding</li> <li>N) Operations Manager: Multi-Service Desk Integration.</li> </ul>

### 10.5.3 System zarządzania incydentami i problemami

Wymaganie	Wymagania dotyczące systemu zarządzania incydentami i problemami
SZliPr	System zarządzania incydentami i problemami musi spełniać następujące wymagania:
SZliPr 1	System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na

	zasoby IT (np. nowa maszyna wirtualna).
SZliPr 2	System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
SZliPr 3	System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
SZliPr 4	System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiającym dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
SZliPr 5	System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać: <ul style="list-style-type: none"> <li>A) Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,</li> <li>B) Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,</li> <li>C) Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,</li> <li>D) Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,</li> <li>E) Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,</li> <li>F) Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,</li> <li>G) Tworzenie baz wiedzy na temat rozwiązywania problemów,</li> <li>H) Automatyzację działań w przypadku znanych i opisanych problemów,</li> <li>I) Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.</li> </ul>

#### 10.5.4 Ochrona antymalware

Wymaganie	Wymagania dotyczące ochrony antymalware
OA	Oprogramowanie antymalware musi spełniać niżej określone wymagania:
OA 1	Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
OA 2	Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem.
OA 3	Centralne zarządzanie politykami ochrony.

OA 4	Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
OA 5	Mechanizmy wspomagające masową instalację.
OA 6	Zastosowanie kilku skanerów antywirusowych różnych producentów na jednej platformie.
OA 7	Możliwość wyboru aktywnych silników skanujących.
OA 8	Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów”, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
OA 9	Aparat ochrony przed złośliwym oprogramowaniem musi używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania.  Aparat ochrony przed złośliwym oprogramowaniem w systemie musi zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
OA 10	Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
OA 11	Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa”, itd.).
OA 12	Pakiet musi umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
OA 13	System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz

	dystrybucji aktualizacji definicji.
OA 14	System ochrony musi mieć możliwość natywnego współdziałania z systemami typu „rights-management”
OA 15	System ochrony musi mieć możliwość filtrowania i blokowania zabronionych przez polityki treści czy słów kluczowych.

## 10.6 Licencje dostępne do serwerowego systemu operacyjnego (na użytkownika)

Licencje dostępne pozwalające użytkownikom korzystać dożywotnio z funkcji serwerowego systemu operacyjnego.

## 10.7 Klientki pakiet antywirusowy

Wymaganie	Minimalne wymagania dotyczące Klientkiego pakietu antywirusowego
KPA	Klientki pakiet antywirusowy musi spełniać poniższe wymagania:
KPA 1	Oprogramowanie licencjonowane na stację roboczą lub serwer.
KPA 2	Ochrona stacji klientki przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
KPA 3	Licencjonowanie w postaci subskrypcji w terminie 5 lat od dnia dokonania odbioru końcowego.
KPA 4	Centralne zarządzanie ochroną stacji klientki poprzez konsolę posiadanego pakietu zarządzania.
KPA 5	Centralne zarządzanie politykami ochrony stacji klientki.
KPA 6	Automatyzacja wymiany dotychczasowych agentów ochrony stacji klientki.
KPA 7	Mechanizmy wspomagające masową instalację.
KPA 8	Zastosowanie kilku skanerów antywirusowych różnych producentów na jednej platformie.
KPA 9	Możliwość wyboru aktywnych silników skanujących.
KPA 10	Pakiet musi wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów”, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania.  Dzięki użyciu technologii minifiltrów, system musi wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie

	minimalizując zaangażowanie użytkownika końcowego.
KPA 11	<p>Aparat ochrony przed złośliwym oprogramowaniem musi używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania.</p> <p>Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.</p>
KPA 12	Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
KPA 13	Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo naszej firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa”, itd.).
KPA 14	Pakiet musi umożliwiać zdefiniowanie jednej zasady konfiguruje technologie antyspieszające, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
KPA 15	System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.
KPA 16	System musi posiadać możliwość natywnego współdziałania z systemami typu „rights-management”.
KPA 17	System musi posiadać możliwość filtrowania i blokowania zabronionych przez polityki treści czy słów kluczowych.



## 10.8 Serwer portalu Internetowego

Wymaganie	Minimalne wymagania dotyczące Serwera Portalu Internetowego
SPI 1	Serwer portalu internetowego musi umożliwiać stworzenie i kompleksowe zarządzanie portalem internetowym. System musi umożliwić zarządzanie i dostęp do treści portalu przez wielu użytkowników, zgodnie z ich uprawnieniami. Wszystkie funkcjonalności związane z administracją portalem oraz dostępem do treści portalu muszą być realizowane przez przeglądarkę Internetową.
SPI 2	Portal musi współpracować z bazą danych, w której przechowuje wszystkie informacje i treści publikowane w portalu.
SPI 3	Serwer portalu internetowego musi umożliwiać publikację dokumentów, treści, plików do ściągnięcia i materiałów multimedialnych na witrynach.
SPI 4	Serwer portalu internetowego musi umożliwiać zarządzanie strukturą portalu i treściami WWW.
SPI 5	Serwer portalu internetowego musi poprawnie publikować obsługiwać treści zbudowane w oparciu o HTML, XML (+XSLT) i PHP w najnowszych wersjach.
SPI 6	Serwer portalu internetowego musi umożliwiać udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z wykorzystaniem praw dostępu na bazie usługi katalogowej.
SPI 7	Serwer portalu internetowego musi umożliwiać uczestnictwo uprawnionych użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści.
SPI 8	Serwer portalu internetowego musi umożliwiać udostępnienie formularzy elektronicznych.
SPI 9	Serwer portalu internetowego musi umożliwiać tworzenie repozytoriów szablonów dokumentów i repozytoriów dokumentów.
SPI 10	Serwer portalu internetowego musi umożliwiać wspólną, bezpieczną pracę nad dokumentami.
SPI 11	Serwer portalu internetowego musi umożliwiać wersjonowanie dokumentów (dla wersji roboczych).
SPI 12	Serwer portalu internetowego musi umożliwiać dołączanie do dokumentów podpisów elektronicznych (jedno- i wielokrotnych).

SPI 13	Serwer portalu internetowego musi umożliwiać wyszukiwanie treści.
SPI 14	Serwer portalu internetowego musi umożliwiać przechowywanie danych w relacyjnej bazie danych.
SPI 15	Serwer portalu internetowego musi umożliwiać wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning).
SPI 16	Serwery WPI(Wielofunkcyjne Portale Internetowe) muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór WIELU niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane i przeglądane niezależnie.
SPI 17	WPI muszą udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu publikacji treści oraz umożliwić współpracę pomiędzy zespołami złożonych również z osób spoza organizacji oraz z jednostek stowarzyszonych.
SPI 18	Serwery WPI muszą posiadać niżej wymienione cechy:
SPI 19	<p><u>Interfejs użytkownika:</u></p> <p>A) Zarządzanie strukturą portalu, rolami użytkowników, uprawnieniami, okresem publikacji treści, tworzenie artykułów.</p> <p>B) Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji uproszczonej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).</p>
SPI 20	<p><u>Integracja</u></p> <p>A) Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili, również do użytkowników z Internetu,</p> <p>B) Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.</p> <p>C) Możliwość wykorzystania mechanizmu jednokrotnej identyfikacji (single sign-on), także z wykorzystaniem SAML 2.0.</p> <p>D) Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym.</p>
SPI 21	Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej

	<p>przez autorów treści:</p> <ul style="list-style-type: none"> <li>A) Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.</li> <li>B) Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów (stron HTML).</li> <li>C) Spójne zarządzanie wyglądem stron, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego.</li> <li>D) Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron i przechowywanymi w repozytorium. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów.</li> <li>E) Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach portalu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte.</li> </ul>
SPI 22	<p><u>Organizacja i publikacja treści:</u></p> <ul style="list-style-type: none"> <li>A) Wersjonowanie treści stron, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.</li> <li>B) Zastosowanie procesów zatwierdzania zawartości przed publikacją, tzn. udostępnieniem jej dla szerokiego grona odbiorców. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed udostępnieniem jej wszystkim użytkownikom.</li> <li>C) Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.</li> <li>D) Automatyczne tworzenie nawigacji na stronach, odwzorowujące</li> </ul>

	<p>obecną hierarchię. Automatyczne generowanie mapy stron portalu.</p> <p>E) Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron portalu. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji. Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu.</p> <p>F) Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.</p>
SPI 23	<p><u>Repozytoria dokumentów</u> muszą posiadać:</p> <p>A) Możliwość prostej publikacji dokumentów.</p> <p>B) Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu.</p> <p>C) Możliwość publikacji plików w strukturze katalogów.</p> <p>D) Możliwość publikacji materiałów wideo oraz audio.</p> <p>E) Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku.</p> <p>F) Możliwość nawigacji po repozytorium dokumentów w oparciu o metadane z metryk dokumentów.</p> <p>G) Prosty mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania.</p> <p>H) Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x... 2.0), automatyczna kontrola wersji przy publikacji dokumentów.</p> <p>I) Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu.</p> <p>J) Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.</p>
SPI 24	<p><u>Wyszukiwanie treści</u> musi umożliwiać:</p> <p>A) Pełnotekstowe indeksowanie zawartości w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez web-service.</p>

	<ul style="list-style-type: none"> <li>B) Centralny mechanizm wyszukiwania treści dostępny dla użytkowników, z uwzględnieniem ich uprawnień.</li> <li>C) Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, dat publikacji.</li> <li>D) Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów portalu wg zadanych kryteriów, np. wg typów dokumentów.</li> <li>E) Możliwość definiowania słownika słów wykluczonych (często używanych).</li> <li>F) Statystyki wyszukiwanych fraz.</li> </ul>
SPI 25	<p><u>Administracja portalem i inne funkcjonalności</u></p> <ul style="list-style-type: none"> <li>A) Możliwość definiowania ról / grup uprawnień w ramach, których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami przez prosty interfejs, niewymagający szczególnych kompetencji technicznych.</li> <li>B) Możliwość implementacji funkcjonalności Single Sign-On.</li> <li>C) Możliwość określania uprawnień do poszczególnych elementów zawartości portalu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu.</li> <li>D) Możliwość zdefiniowania uprawnień dostępu do całego portalu opartego o serwer portalu internetowego lub do poszczególnych sekcji portalu na poziomach: dostęp publiczny, dostęp dla użytkowników wewnętrznych, wg uprawnień nadawanych przez centralnego administratora lub uprawnionych administratorów.</li> <li>E) Generowanie konfigurowalnych powiadomień pocztą elektroniczną dla użytkowników z informacją o publikacji najbardziej istotnych treści.</li> <li>F) Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu.</li> <li>G) Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów.</li> <li>H) Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów portalu.</li> <li>I) Statystyki odwiedzin poszczególnych części i stron portalu – analiza</li> </ul>

	<p>liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy.</p> <p>J) Funkcjonalności wspierające pracę grupową – wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń.</p> <p>K) Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.</p> <p>L) Funkcjonalność definiowania procesów obiegu dokumentów (workflow) przy wykorzystaniu prostych w obsłudze narzędzi portalu.</p>
--	--

## 10.9 Serwer relacyjnej bazy danych

	Serwer relacyjnej bazy danych
Wymaganie	Minimalne wymagania dotyczące Serwera relacyjnej bazy danych
SRBD 1	Serwer relacyjnej bazy danych (RBD) musi spełniać poniższe wymagania poprzez wbudowane mechanizmy:
SRBD 2	<p><u>Możliwość szyfrowania przechowywanych danych</u></p> <p>System RBD musi pozwalać na szyfrowanie przechowywanych danych. Szyfrowanie musi być cechą systemu RBD i nie może wymagać jakichkolwiek zmian w aplikacjach korzystających z danych. Zasyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zaszyfrowana.</p>
SRBD 3	<p><u>Kompresja kopii zapasowych</u></p> <p>System RBD powinien pozwalać na kompresję kopii zapasowej danych (<i>backup</i>) od razu w czasie jej tworzenia. Powinna to być cecha RBD niezależna od systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.</p>
SRBD 4	<p><u>Ograniczenie użycia zasobów</u></p> <p>System powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, pamięć). Reguły definiujące ograniczenia użytkowników lub ich grup w wykorzystaniu zasobów powinny mieć możliwość użycia w nich logiki zaimplementowanej za pomocą języka programowania (np. używanego w danym RBD języka SQL).</p>
SRBD 5	<p><u>Korzystanie z zewnętrznych urządzeń do przechowywania kluczy szyfrujących</u></p> <p>RBD powinien posiadać mechanizm pozwalający na i przechowywanie kluczy szyfrujących na urządzeniach zewnętrznych (np. czytniki kart). Rozwiązanie to powinno być otwarte, to znaczy pozwalać na dodawanie w przyszłości obsługi</p>

	urządzeń nowych, oczywiście pod warunkiem dostarczenia przez producenta urządzenia odpowiednich modułów oprogramowania zgodnych z RBD.
SRBD 6	<p><u>Skalowalność systemu</u></p> <p>System RBD powinien wspierać skalowanie w kontekście wielkości rozwiązania (powinien być dostępny zarówno na platformie wielo-serwerowej, jak również średniej wielkości komputerów i urządzeń mobilnych).</p>
SRBD 7	<p><u>Możliwość zastosowania reguł bezpieczeństwa obowiązujących w jst.</u></p> <p>Wsparcie dla zdefiniowanej w jst polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników lub zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników).</p>
SRBD 8	<p><u>Możliwość definiowania zasad administracyjnych dla serwera lub grupy serwerów</u></p> <p>System RBD powinien mieć możliwość automatyzacji zadań administracyjnych przez definiowanie reguł wymuszanych potem przez system. Przykłady takich reguł:</p> <ul style="list-style-type: none"> <li>A) uniemożliwienie użytkownikom tworzenia obiektów (np. tabel, procedur, baz danych, widoków) o zdefiniowanych przez administratora nazwach lub ich fragmentach.</li> <li>B) Powinna być możliwa rejestracja i raportowanie niezgodności ze wskazanymi regułami działającego systemu bez wpływu na jego funkcjonalność.</li> </ul> <p>Reguły mogą dotyczyć serwera lub grupy serwerów.</p>
SRBD 9	<p><u>Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym</u></p> <p>System RBD powinien pozwalać na definiowanie rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych bez ujemnego wpływu na wydajność rozwiązania. Przykłady takich zdarzeń to:</p> <ul style="list-style-type: none"> <li>A) odczyt lub zapis danych na dysku dla wyszczególnionego zapytania (w celu wychwytywania zapytań znacząco obciążających system),</li> <li>B) wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),</li> <li>C) para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy takim jak np. tabela (w celu wychwytywania długotrwałych blokad obiektów bazy).</li> </ul> <p>Rejestracja zdarzeń powinna pozwalać na selektywne ich wychwytywanie (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu).</p>
SRBD 10	<p><u>Możliwość rejestracji zmiany w rekordzie danych</u></p> <p>System powinien pozwalać na rejestrację zmian w danych włącznie z zapamiętaniem</p>

	<p>stanu pojedynczego rekordu danych sprzed modyfikacji. Rozwiązanie nie powinno ujemnie wpływać na wydajność systemu i powinno być konfigurowalne bez wpływu na istniejące aplikacje korzystające z danych. Rozwiązanie powinno rejestrować także zmiany w definicji struktur danych (np. zmiany schematu tabeli).</p>
SRBD 11	<p><u>Audyt dostępu do danych</u></p> <p>System RBD powinien pozwalać na rejestrację operacji takich jak: logowanie, wylogowanie użytkownika, zmiany w definicji obiektów bazy danych (tabele, procedury), wykonywanie przez wskazanego użytkownika operacji takich jak SELECT, INSERT, UPDATE, DELETE. Rozwiązanie powinno być niezależne od aplikacji, wbudowane w RBD.</p>
SRBD 12	<p><u>Zarządzanie serwerem za pomocą skryptów</u></p> <p>System RBD powinien udostępniać mechanizm zarządzania silnikiem bazy danych za pomocą skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.</p>
SRBD 13	<p><u>Możliwość dodawania procesorów bez restartu systemu</u></p> <p>System RBD powinien umożliwiać dodanie procesora do systemu bez konieczności restartu silnika bazy danych.</p>
SRBD 14	<p><u>Możliwość dodawania pamięci bez restartu systemu</u></p> <p>System RBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych.</p>
SRBD 15	<p><u>Możliwość wywoływania procedur składowanych jako usług sieci Web (WebServices)</u></p> <p>System RBD powinien umożliwiać tworzenie procedur składowanych które mogą być udostępnione i wywoływane jako <i>WebServices</i> bez wykorzystania dodatkowego oprogramowania.</p>
SRBD 16	<p><u>Kopie bazy tylko do odczytu</u></p> <p>System powinien umożliwiać tworzenie w dowolnym momencie kopii tylko do odczytu bazy danych z bieżącego momentu czasu. Wiele takich kopii może być równolegle użytkowanych w celu wykonywania z nich zapytań.</p>
SRBD 17	<p><u>Wysoka dostępność realizowana programowo z korekcją błędów pamięci masowej</u></p> <p>System RBD powinien posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:</p> <p style="padding-left: 40px;">A) bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam RBD),</p>



	<p>B) niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),</p> <p>C) klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,</p> <p>D) czas przełączenia na system zapasowy poniżej 10 sekund,</p> <p>E) brak limitu odległości między systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza),</p> <p>F) kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenia sieci),</p> <p>G) system automatycznie naprawia błędy pamięci masowej (w przypadku odkrycia błędu fizycznego odczytu danych z pamięci masowej, poprawny fragment danych jest transferowany z drugiego systemu i korygowany).</p> <p>System RBD powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych.</p>
SRBD 18	<p><u>Wykonywanie typowych zadań administracyjnych w trybie on-line</u></p> <p>System RBD powinien umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy (operacje w trybie on-line).</p>
SRBD 19	<p><u>Definiowanie nowych typów danych w RBD</u></p> <p>System RBD powinien umożliwiać definiowanie nowych typów danych wraz z definicją specyficzną dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.</p>
SRBD 20	<p><u>Wsparcie dla technologii XML</u></p> <p>System RBD powinien udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności powinien:</p> <p>A) udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,</p> <p>B) udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,</p> <p>C) udostępniać język zapytań do struktur XML,</p> <p>D) udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),</p>

	E) udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.
SRBD 21	<p><u>Obsługa błędów w kodzie zapytań</u></p> <p>Język zapytań i procedur w systemie RBD powinien umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.</p>
SRBD 22	<p><u>Możliwość tworzenia rekursywnych zapytań do bazy danych.</u></p> <p>System RBD powinien udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.</p>
SRBD 23	<p><u>Replikacja danych i modyfikacja w wielu punktach</u></p> <p>System RBD powinien pozwalać na transakcyjną replikację wybranych danych z bazy danych między wieloma węzłami. Dodanie lub usunięcie węzła nie powinno wpływać na funkcjonowanie i spójność systemu replikacji ani nie powinno przerywać procesu replikacji. Dane mogą w takim schemacie replikacji być modyfikowane w dowolnym węźle (ale tylko w jednym węźle w danym momencie). System powinien zawierać narzędzie do nadzorowania i wizualizacji topologii oraz stanu procesu replikacji.</p> <p>Dodatkowo system RBD powinien umożliwiać kompresję przesyłanych danych między serwerami uczestniczącymi w replikacji, aby minimalizować obciążenie łącz sieciowych.</p>
SRBD 24	<p><u>Indeksowanie podzbioru danych w tabeli</u></p> <p>System RBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.</p>
SRBD 25	<p><u>Dedykowana sesja administracyjna</u></p> <p>System RBD powinien pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.</p>
SRBD 26	<p><u>Partycjonowanie danych</u></p> <p>System powinien pozwalać na podział danych w jednej tabeli między różne fizyczne pamięci masowe zgodnie ze zdefiniowanymi warunkami podziału.</p> <p>System RBD powinien udostępniać mechanizm równoległego (wielowątkowego) dostępu do danych umieszczonych w różnych partycjach.</p> <p>Dodatkowo powinna być dostępna możliwość szybkiego przesyłania dużych zbiorów danych poprzez mechanizm przełączania partycji (czyli dane przenoszone są z jednej tabeli do drugiej za pomocą operacji na metadanych, a nie przez fizyczne</p>

	<p>kopiowanie rekordów). Dzięki takiej funkcjonalności możliwe jest przeniesienie dużej liczby rekordów w bardzo krótkim czasie (rzędu sekund). Dodatkowo minimalizowane jest odczuwanie wpływu tej operacji przez użytkowników (minimalny wpływ przenoszenia danych na obciążenie systemu).</p>
SRBD 27	<p><u>Możliwość efektywnego przechowywania dużych obiektów binarnych</u></p> <p>System RBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty, itp.)</p> <p>Obiekty te nie powinny być przechowywane w plikach bazy danych, ale w systemie plików. Jednocześnie pliki te powinny być zarządzane przez RBD (kontrola dostępu na podstawie uprawnień nadanych w RBD). Dodatkowo dane binarne powinny być dostępne dla użytkowników bazy danych jako standardowa kolumna tabeli (dostęp z poziomu zapytań języka SQL obsługiwanego przez RBD).</p>
SRBD 28	<p><u>Możliwość kompresji przechowywanych danych</u></p> <p>System RBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych.</p> <p>Ze względu na to, że wydajność serwerów baz danych w największym stopniu ograniczana jest przez podsystemy dyskowe, zastosowanie kompresji danych pozwoli osiągnąć lepszą wydajność przy nie zmienionej konfiguracji sprzętowej (skompresowane dane zajmują mniej miejsca, a skoro zajmują mniej miejsca, to ich odczytanie zajmuje mniej zasobów).</p> <p>System kompresji powinien umożliwiać również kompresję UNICODE systemem UCS-2.</p>
SRBD 29	<p><u>Raportowanie zależności między obiektami</u></p> <p>System RBD powinien udostępniać obiekty systemowe do raportowania zależności między obiektami baz danych. Mechanizm ten powinien umożliwiać m.in. uzyskanie informacji o referencjach między obiektami, czyli które obiekty bazy danych odwołują się do innych obiektów.</p>
SRBD 30	<p><u>Mechanizm blokowania planów wykonania zapytań do bazy danych</u></p> <p>System RBD powinien udostępniać mechanizm pozwalający na zablokowanie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Ma to istotne znaczenie m.in. w przypadku przenoszenia systemów między serwerami (środowisko testowe i produkcyjne), migracji do innych wersji RBD lub wprowadzania zmian sprzętowych w serwerach.</p> <p>Dzięki mechanizmom blokady planów wykonania zapytań czas odpowiedzi na zapytania staje się bardziej przewidywalny.</p>



SRBD 31	<p><u>Efektywne zarządzanie pustymi wartościami w bazie danych</u></p> <p>System RBD powinien efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.</p>
SRBD 32	<p><u>Wsparcie dla optymalizacji zapytań z modelu gwiazdy (fakty-wymiary)</u></p> <p>System RBD powinien udostępniać mechanizmy optymalizacji zapytań w modelu gwiazdy (tabela faktów łączona z tabelami wymiarów). Zapytania te często wykorzystywane są w hurtowniach danych i analizach wielowymiarowych. Ze względu na dużą liczbę danych wykorzystywanych w tego typu zapytaniach metody optymalizacji tego typu zapytań pozwalają znacząco zwiększyć wydajność przy tworzeniu rozwiązań hurtowni danych i wielowymiarowych struktur analitycznych (OLAP).</p>
SRBD 33	<p><u>Wsparcie dla Indeksów kolumnowych</u></p> <p>System RBD powinien umożliwiać tworzenie indeksów przechowujących dane osobno dla każdej z kolumn tabeli łącząc je następnie w całość. Indeks powinien również wykorzystywać mechanizm kompresji.</p>
SRBD 34	<p><u>Wsparcie dla zapytań aktualizujących tabele faktów w modelach wielowymiarowych</u></p> <p>System RBD powinien udostępniać wbudowane mechanizmy pozwalające w łatwy i szybki sposób aktualizować zawartość tabel faktów (wykorzystywanych w modelach wielowymiarowych). Mechanizm ten powinien być dostępny z poziomu zapytań języka SQL obsługiwanych przez silnik bazy danych.</p>
SRBD 35	<p><u>System transformacji danych</u></p> <p>System powinien posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Zestaw standardowych dostępnych transformacji powinien obejmować takie transformacje jak: sortowanie, wyszukiwanie wartości według klucza w tabelach słownikowych, automatyczna obsługa SCD (<i>Slowly Changing Dimension</i>) w zasilaniu hurtowni danych, pobranie danych z serwera FTP, wysłanie e-maila, łączenie danych z wykorzystaniem logiki rozmytej, poprawa jakości danych wykorzystująca integrację z dedykowanym systemem zarządzania jakością danych oraz jego bazą wiedzy i reguł walidujących. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.</p>



	<p>A) mechanizm debuggowania tworzonego rozwiązania,</p> <p>B) mechanizm stawiania „pułapek” (breakpoints),</p> <p>C) mechanizm logowania do pliku wykonywanych przez transformację operacji,</p> <p>D) możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),</p> <p>E) możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo),</p> <p>F) mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),</p> <p>G) mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),</p> <p>H) mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,</p> <p>I) mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiiany źródła danych.</p> <p>Wykonywane transformacje danych powinny mieć możliwość integracji z transakcjami bazy danych RBD, także rozproszonymi (transakcje obejmujące bazy na różnych fizycznych serwerach RBD) bez potrzeby pisania kodu.</p>
SRBD 36	<p><u>System analityczny</u></p> <p>A) System powinien posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych).</p> <p>B) System powinien umożliwiać pracę w dwóch trybach:</p> <ol style="list-style-type: none"> <li>wielowymiarowym (tworzenie kostek wielowymiarowych),</li> <li>tabelarycznym (wykorzystującym technologię in-memory BI).</li> </ol> <p>Powinno być możliwe tworzenie: wymiarów, miar.</p> <p>Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo-&gt;Gmina.</p> <p>C) System powinien mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP</p>



	<p>– wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna powinna mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Agregacje powinny być przeliczane niezależnie dla każdego modelu składowania w jednej bazie.</p> <p>D) System powinien pozwalać na integrację z RBD – wymagana jest możliwość uruchomienia procesu wyliczenia agregacji zainicjowana poprzez dodanie rekordu do tabeli w RBD. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).</p> <p>E) System powinien pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron WWW powiązanych z przeglądany obszarem kostki).</p> <p>F) System powinien posiadać narzędzie do rejestracji i śledzenia wykonywanych zapytań spójne z analogicznym narzędziem dla systemu RBD.</p> <p>G) System powinien umożliwiać rejestrowanie zapytań wykonywanych przez użytkowników, a następnie umożliwiać na podstawie zgromadzonych informacji na automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).</p> <p>H) System powinien obsługiwać wielojęzykowość (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).</p> <p>I) System powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.</p> <p>J) System powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.</p> <p>K) System powinien umożliwiać użytkownikom tworzenie analiz In-Memory, czyli przetwarzanie dużej liczby rekordów skompresowanych w pamięci RAM. Powinien umożliwiać tworzenie modeli wykorzystujących tabele pochodzące z wielu niezależnych źródeł danych i łączone między sobą relacjami.</p> <p>L) System powinien udostępniać dedykowany język do tworzenia logiki biznesowej w modelu. Język ten powinien m.in. obsługiwać relacje utworzone między tabelami, mechanizmy time intelligence (operacje na</p>
--	---

	<p>datach i okresach) oraz zapewniać mechanizmy kontroli bezpieczeństwa i dostępu do danych na poziomie poszczególnych wierszy.</p> <p>M) System powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane).</p> <p>N) System powinien mieć wbudowaną funkcję importu tabelarycznych modeli danych wykorzystujących technologię in-memory BI i przygotowanych w aplikacji Microsoft Excel. Podczas procesu importu na serwerze model powinien być odtwarzany w postaci bazy danych.</p> <p>O) System powinien umożliwiać zasilanie modelu tabelarycznego m.in. z następujących systemów źródłowych: bazy relacyjne, bazy wielowymiarowe, modele tabelaryczne, zbiory danych przechowywane w usługach chmury publicznej, pliki płaskie, inne raporty udostępniane w formacie Atom 1.0.</p> <p>P) System powinien umożliwiać działanie modelu tabelarycznego w dwóch trybach – z użyciem buforowania (możliwe opóźnienie, ale większa wydajność) oraz bez użycia buforowania (zapytania użytkowników końcowych korzystających z modelu są przesyłane bezpośrednio do źródłowej bazy relacyjnej i zwracają najbardziej aktualną wersję danych).</p> <p>Q) System analityczny powinien udostępniać rozwiązania Data Mining ( m.in. algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), podobieństw sekwencyjnych (Sequence Clustering), sieci neuronowych (Neural Nets) oraz Naive Bayes) oraz możliwość ich integracji ze strukturami wielowymiarowymi. Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.</p> <p>R) System powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.</p>
SRBD 37	<p><u>Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators)</u></p> <p>A) System powinien udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.</p> <p>B) System powinien umożliwiać tworzenie takich wskaźników również w modelach danych wykorzystujących technologię in-memory BI.</p>





SRBD 38	<p><u>Kreatory modelowania złożonych procesów biznesowych</u></p> <p>System powinien udostępniać szereg łatwych w użyciu kreatorów pozwalających niezaaansowanym użytkownikom implementować złożone problemy analizy biznesowej w modelu analitycznym, czyniąc programowanie projektów BI przystępnym dla większej liczby osób i organizacji.</p>
SRBD 39	<p><u>aktywne buforowanie danych w wielowymiarowej bazie danych</u></p> <p>System powinien udostępniać mechanizm odświeżania danych w strukturach wielowymiarowych, który wykrywa zmiany w systemach źródłowych i na bieżąco aktualizuje bazę wielowymiarową.</p>
SRBD 40	<p><u>System raportowania</u></p> <p>A) System RBD powinien posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępniane przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki) bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:</p> <ol style="list-style-type: none"><li>raporty parametryzowane,</li><li>cache raportów (generacja raportów bez dostępu do źródła danych),</li><li>cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych z różnymi wartościami parametrów),</li><li>współdzielenie predefiniowanych zapytań do źródeł danych,</li><li>wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),</li><li>możliwość opublikowania elementu raportu (wykresu, tabeli) do współdzielonej biblioteki, z której mogą korzystać inni użytkownicy, tworząc nowy raport ze znajdujących się w bibliotece elementów raportowych,</li><li>możliwość wizualizacji wskaźników KPI,</li><li>możliwość wizualizacji danych w postaci obiektów sparkline.</li></ol> <p>B) Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).</p> <p>C) Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel (od wersji 1997 do 2010), Microsoft Word (od wersji 1997 do 2010), HTML, TIFF.</p> <p>D) Dodatkowo raporty powinny być eksportowane w formacie Atom Feed, które można będzie wykorzystać jako źródło danych w innych aplikacjach.</p>



	<p>E) System RBD powinien umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.</p> <p>F) System RBD powinien umożliwiać wysyłkę raportów w wybranym formacie (drogą mailową) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).</p> <p>G) System raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.</p>
SRBD 41	<p><u>Narzędzia do tworzenia raportów ad-hoc</u></p> <p>System powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez niezaaansowanych użytkowników. Tworzenie raportów powinno odbywać się w środowisku graficznym. Użytkownicy powinni mieć możliwość na publikowanie stworzonych raportów na serwerze w celu udostępnienia ich szerszemu gronu osób.</p>
SRBD 42	<p><u>Zintegrowanie narzędzia do zarządzania systemem</u></p> <p>System powinien dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te powinny udostępniać możliwość tworzenia i wykonywania skryptów zarządzających RBD oraz silnikiem baz wielowymiarowych OLAP.</p>
SRBD 43	<p><u>Możliwość tworzenia funkcji i procedur w innych językach programowania</u></p> <p>A) System powinien umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego RBD.</p> <p>B) System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy.</p> <p>C) Dodatkowo system powinien udostępniać środowisko do debuggowania.</p>
SRBD 44	<p><u>Możliwość zarządzania centralnymi słownikami danych</u></p> <p>A) System powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM).</p> <p>B) System MDM powinien:</p> <ol style="list-style-type: none"> <li>udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach,</li> </ol>



	<ul style="list-style-type: none"><li>ii. wersjonowanie danych (możliwość śledzenia zmian wprowadzonych przez użytkowników z możliwością ich cofnięcia do wybranej wersji),</li><li>iii. udostępniać mechanizm tworzenia i uruchamiania reguł walidujących poprawność danych w słownikach,</li><li>iv. udostępniać narzędzia do administracji i kontroli uprawnień dostępu do danych w MDM,</li><li>v. udostępniać zestaw bibliotek (API programistyczne) z funkcjonalnościami MDM do wykorzystania w aplikacjach użytkownika,</li><li>vi. umożliwiać eksport danych zgromadzonych w systemie MDM,</li><li>vii. umożliwiać zarządzanie danymi podstawowymi z poziomu programu Microsoft Excel.</li></ul>
SRBD 45	<p><u>Możliwość rejestrowania bardzo dużej liczby zdarzeń i analizowania ich z minimalnym opóźnieniem</u></p> <p>A) System powinien dostarczać wbudowaną platformę do tworzenia aplikacji typu CEP (Complex Event Processing). Aplikacje takie umożliwiają rejestrowanie bardzo dużej liczby zdarzeń i reagowanie na nie z minimalnym opóźnieniem.</p> <p>B) System powinien również udostępniać mechanizmy wysokiej dostępności dla tej usługi.</p>
SRBD 46	<p><u>Narzędzia do zarządzania jakością danych</u></p> <p>System powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:</p> <p>A) udostępniać funkcje do profilowania danych (analiza i raporty dot. jakości danych),</p> <p>B) udostępniać funkcje do deduplikacji danych,</p> <p>C) określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną (którą może ale nie musi zaakceptować użytkownik),</p> <p>D) umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów),</p> <p>E) umożliwiać definiowanie złożonych domen (zestawu kilku atrybutów) oraz ocenę jakości danych na podstawie powiązań między tymi atrybutami (np. weryfikację poprawności danych adresowych złożonych z kodu pocztowego, miasta i ulicy),</p> <p>F) pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania),</p>

---

	<p>G) umożliwiać eksport wyników badania (poprawnych i sugerowanych wartości) do pliku tekstowego lub bazy relacyjnej; eksport powinien obejmować wartości po korekcie (poprawione) oraz ewentualnie te przed korektą (błędne),</p> <p>H) przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy),</p> <p>I) umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych,</p> <p>J) zapewniać mechanizmy „uczenia się” bazy wiedzy – czyli w miarę realizacji kolejnych procesów ręcznego czyszczenia danych baza wiedzy powinna umożliwiać gromadzenie tych informacji na potrzeby kolejnych procesów,</p> <p>K) umożliwiać wykorzystanie bazy wiedzy w automatycznym procesie czyszczenia danych (powinien integrować się z narzędziami do ekstrakcji, transformacji i ładowania danych, dzięki czemu będzie można wykorzystać te mechanizmy w automatycznym procesie ładowania danych.</p>
--	---

## 11 Infrastruktura sieciowa oraz sprzętowa SeUI w Urzędzie Marszałkowskim

Celem budowy infrastruktury sieciowej w SeUI w Urzędzie Marszałkowskim jest przygotowanie wydajnej i bezpiecznej platformy sprzętowo-programowej dla obsługi ruchu pochodzącego zarówno od użytkowników zewnętrznych jak i wewnętrznych. Infrastruktura powinna być zbudowana zgodnie z obowiązującymi dzisiaj trendami w zakresie projektowania i zabezpieczania takich systemów informatycznych oraz uwzględniać zapas wydajności na przyszłe potrzeby związane z tworzoną systemem.

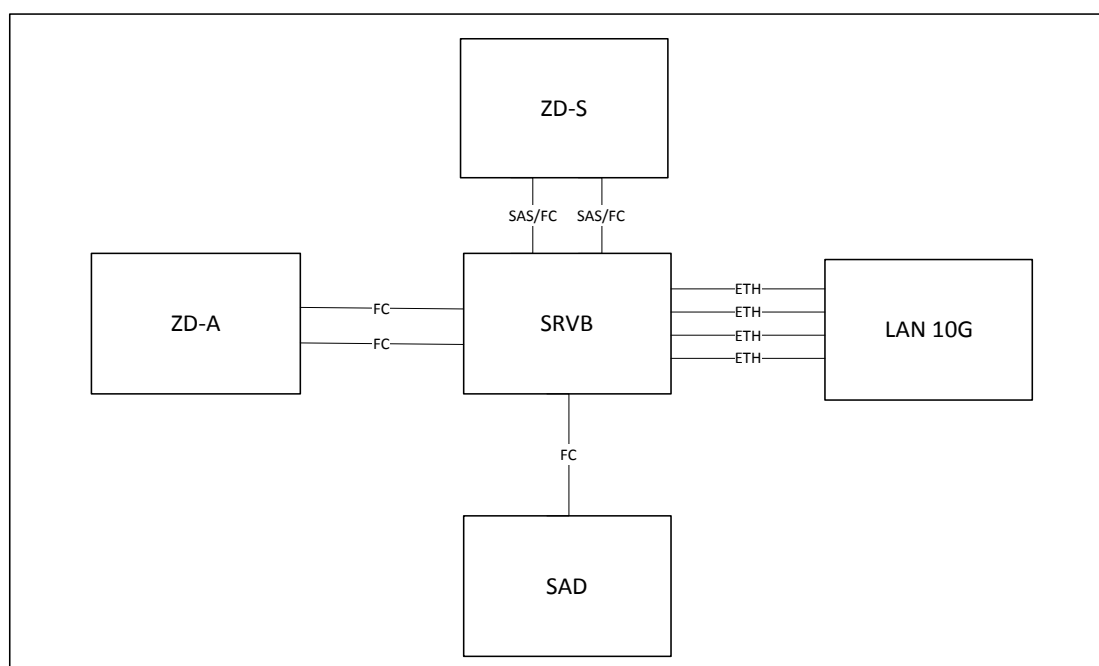
Przygotowana koncepcja zakłada możliwość instalacji urządzeń sieciowych w szafach rackowych oraz pełną redundancję wszystkich urządzeń sieciowych wykorzystanych w strukturze. Redundancję stosuje się w celu zmniejszenia prawdopodobieństwa załamania pracy systemu i w przypadku niniejszego projektu polega na zdublowaniu krytycznych elementów systemu (m.in. serwerów).

Założono, że wszystkie zaplanowane dla SeUI urządzenia będą znajdować się w jednej geograficznie lokalizacji tj. w serwerowni Urzędu Marszałkowskiego. Przygotowane zestawienie sprzętu zakłada dodatkowo redundancję wszystkich zasilaczy urządzeń sieciowych. Aby efektywnie wykorzystać tą funkcjonalność założono, że serwerownia będzie posiadała co najmniej dwa niezależne tory zasilające.

### 11.1 Dostawa sprzętu i urządzeń

Poniżej przedstawione zostały wymagane minimalne wartości parametrów omawianych urządzeń.

#### 11.1.1 Oznaczenia i definicje



---

### Rysunek 3 Poglądowy schemat architektury systemu

Schemat blokowy, oznaczenia i skróty literowe:

SRVB – Serwer Blade

ZD-S – Zasób Dyskowy Systemowy

ZD-A – Zasób Dyskowy Aplikacji

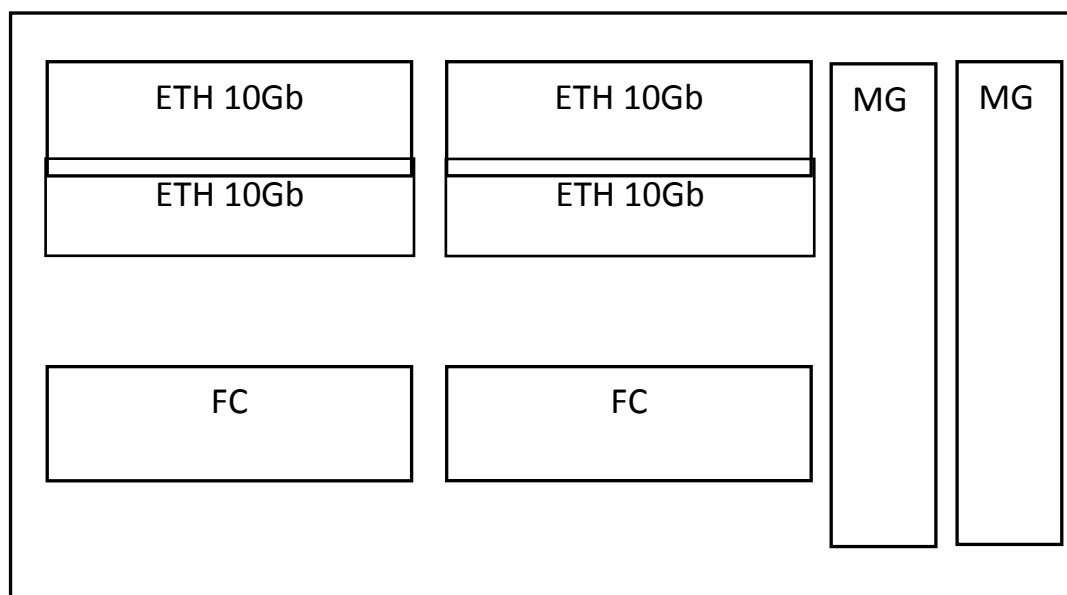
SAD – System Archiwizacji Danych

SAS/FC – Połączenie FIBRE CHANNEL lub SAS o przepustowości co najmniej 6Gb/s

FC – połączenie FIBRE CHANNEL o przepustowości co najmniej 8Gbit/s

ETH – połączenie ETHERNET o przepustowości co najmniej 10GB

LAN 10G – przełączniki ETHERNET 10G sieci LAN



Rysunek 4 Poglądowy schemat rozmieszczenia PRZEŁACZNIKÓW w Obudowie BLADE

Oznaczenia:

ETH 10Gb      Przełącznik BLADE ETHERNET 10Gb

SAS/FC        Przełącznik BLADE, SAS lub FC

MG             Moduł Zarządzający

### Definicja BLADE

Dla potrzeb niniejszej specyfikacji Zamawiający jako BLADE dopuszcza wyłącznie takie rozwiązania, które określane są w swoich nazwach handlowych jako rozwiązania BLADE.

Ponadto muszą spełniać równocześnie następujące warunki:

- a) serwery wraz z przełącznikami muszą posiadać wspólną obudowę z nadmiarowym oraz wymiennym podczas pracy systemem zasilania i chłodzenia,
- b) serwery oraz przełączniki muszą komunikować się znajdującą się wewnątrz obudowy BLADE magistralą redukując zewnętrzne okablowanie,
- c) obudowa BLADE musi posiadać port do zarządzania, który stanowi wspólne źródło do zarządzania infrastrukturą BLADE (serwery, zasilanie, chłodzenie, przełączniki (za wyjątkiem przełączników nie posiadających wewnętrznego systemu zarządzania)) dostępne pod jednym adresem, jednym identyfikatorem oraz hasłem.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego technologia blade jest oznaczana dużymi literami (BLADE) w odróżnieniu od innych technologii blade.

### Standaryzacja przepustowości

W celu uniknięcia nieporozumień związanych z pojęciem przepustowości, które użyte jest w późniejszym tekście wymagań Zamawiający podaje wartości, które należy przyjąć przy obliczaniu przepustowości na potrzeby niniejszej specyfikacji.

**Tabela 1. Zestawienie Przepustowości**

standard	Przepustowość [Gb/s]
DDR3-1066 ; -1333 ; -1600	8,5 ; 10,6 ; 12,8 [GB/s]
10 Gb Ethernet ; 1 Gb Ethernet	10 ; 1
8 Gb ; 4 Gb FC	8 ; 4
QDR ;DDR ; SDR InfiniBand	10 ; 5 ; 2,5
EDR ; FDR InfiniBand	26 ; 14
6G ; 3G SAS	6 ; 3
6G ; 3G ; 1,5 SATA	6 ; 3 ; 1,5

Jeśli port używa zwielokrotnionych linii jego przepustowość na potrzeby niniejszej specyfikacji należy przyjąć jako iloczyn liczby linii i wyżej podanej przepustowości (przykład: przepustowość 4X QDR INFINIBAND na potrzeby niniejszej specyfikacji wynosi 40 Gb/s).

Jeśli transmisja na linii zachodzi równocześnie w dwu kierunkach to dla potrzeb niniejszej specyfikacji należy przyjąć nie wartość dwukrotnie wyższą, ale dokładnie taką jaką znajduje się podanej tabeli.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego przepustowość, a opisana w niniejszym akapicie jest oznaczana dużą literą (PRZEPUSTOWOŚĆ) w odróżnieniu od innych przepustowości.

### Równoważność kanałów komunikacyjnych

I) W miejscach gdzie Zamawiający wyspecyfikował rodzaj kanału komunikacyjnego jako równoważny kanał komunikacyjny Zamawiający dopuszcza kanał komunikacyjny o identycznym protokole, ale o większej prędkości. Zamawiający nie dopuszcza innego niż wyspecyfikowany protokołu pomimo, że zamienny protokół będzie posiadał większą przepustowość. Przykład:

- a) Dla wymagania ETHERNET 10Gb jako równoważne NIE JEST akceptowane połączenie o większej przepustowości, ale jedynie o większej prędkości. W tym wypadku ETHERNET 100Gb.
- b) Analogicznie dla wymagania FC 8Gb jako równoważne akceptowane jest jedynie połączenie FC, ale o większej prędkości. W tym wypadku FC 16Gb lub więcej.

### **Definicja pojęcia MOC OBLICZENIOWA**

Wzór 1. Maksymalna (szczytowa) teoretyczna moc obliczeniowa procesora

$$R_{proc} = C * I * F,$$

gdzie:

$R_{proc}$  - moc obliczeniowa w GFlops

C - liczba rdzeni procesora

I - liczba instrukcji zmiennoprzecinkowych typu dodawanie i mnożenie w podwójnej precyzji wykonywanych przez pojedynczy rdzeń procesora w czasie jednego cyklu zegarowego (np. dla procesora Intel Xeon (seria 5600) I wynosi 4, dla procesorów AMD Opteron I wynosi 4),

F - częstotliwość zegara procesora w GHz.

Dla potrzeb niniejszej specyfikacji Zamawiający jako częstotliwość zegara przyjmuje nominalną częstotliwość zegara procesora podawaną przez producenta procesora przy handlowym opisie procesora. Pomimo, że procesor może pracować z częstotliwością niższą lub wyższą niż wyżej wspomniana częstotliwość jako częstotliwość do obliczenia mocy obliczeniowej procesora w niniejszej specyfikacji należy przyjąć właśnie częstotliwość podawaną przy opisach handlowych przez producentów procesorów.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego moc obliczeniowa zdefiniowana we wzorze 1 i opisana w niniejszym akapicie jest oznaczana dużą literą (moc obliczeniowa) w odróżnieniu od innych mocy obliczeniowych.

### **Definicja ZASÓB DYSKOWY**

Dla potrzeb niniejszej specyfikacji jako zasób dyskowy Zamawiający dopuszcza każde urządzenie które dodatkowo równocześnie spełnia następujące właściwości:

- a) dyski znajdują się wewnątrz urządzenia,

- b) dyski połączone są znajdującą się wewnątrz urządzenia magistralą połączeń do wspólnych portów wejścia / wyjścia urządzenia,
- c) wymagana magistrala połączeń nie jest w postaci kabli dostępnych z zewnątrz,
- d) na zewnątrz urządzenia dostępne jedynie są porty wejścia / wyjścia, do których dołącza się kable sygnałowe do transmisji pomiędzy dyskami, a pozostałą częścią infrastruktury, jeśli takie połączenie jest wymagane.

W zapisach niniejszej specyfikacji tak określone urządzenie jest „Zasobem dyskowym” i oznaczana jest dużą literą w odróżnieniu od innych urządzeń.

### Konwencja zapisów

- I) Zapis „SAS / FC” lub „USB / SD” użyty w dalszej części specyfikacji oznacza jedną z dwóch technologii: albo SAS albo FC, albo USB albo SD.
- II) Nazwy pisane z dużej litery są stosowanymi na potrzeby niniejszej specyfikacji nazwami własnymi np. Serwer BLADE, Lokalne Dyski.
- III) Słowa „LUB” lub „ALBO” napisane z dużej litery oznaczają kwalifikator logiczny i nie są używane w potocznym znaczeniu.

Przykład:

- a) Jeśli Zamawiający wymaga odporności Systemu na awarię elementu A ALBO elementu B oznacza to, że System nie musi być odporny na RÓWNOCZESNĄ awarię elementu A i elementu B.
- b) Jeśli Zamawiający wymaga odporności systemu na awarię elementu A LUB elementu B oznacza to, że system nie tylko ma być odporny na awarię jednego z dwu elementów A albo B, ale też musi być odporny na równoczesną awarię obu elementów: i A i B.

### Jakość sprzętu

- a) Cały dostarczony sprzęt musi być fabrycznie nowy, tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów jego poprawnej pracy.
- b) Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.

## 11.2 Wymagania sprzętowe –szczegółowe

### 11.2.1 Obudowa Blade

Parametr	Charakterystyka (wymagania minimalne) Obudowa Blade
OB 1	Wykonawca ma dostarczyć 1 parę (2 szt.) lub więcej par identycznych i identycznie wyposażonych Obudów BLADE (identyczne modele i ilości: serwerów, przełączników BLADE, zasilaczy, wiatraków oraz zarządzania):



OB 2	W każdej obudowie BLADE musi zostać zainstalowana taka sama, parzysta, ilość serwerów BLADE.
OB 3	Musi istnieć możliwość wymiany Serwerów BLADE pomiędzy zaoferowanymi obudowami BLADE.
OB 4	W razie awarii jednej z zaoferowanych obudów BLADE musi istnieć możliwość instalacji wszystkich serwerów w pozostałych zaoferowanych obudowach BLADE.
OB 5	<p>A) 8 szt. lub więcej zatok na serwery BLADE.</p> <p>B) 5 szt. lub więcej zatok na moduły przełączników.</p> <p>C) obudowa w standardzie RACK dopasowana do dostarczanej szafy.</p>
OB 6	<p>Nadmiarowy, odporny na awarię 1 szt. zasilacza albo 1 szt. wiatraka -system, który spełnia następujące wymagania:</p> <p>A) Wymienny z zewnątrz, podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</p> <p>B) W ilości maksymalnej dla obudowy BLADE przewidzianej przez producenta obudowy. Tak by w razie rozbudowy nie było konieczności dokupowania elementów infrastruktury.</p>
OB 7	<p>Wymaga się działania następujących właściwości</p> <p>A) Zintegrowany i złożony z 2 szt. gotowych do pracy, identycznych modułów system zarządzania. W razie awarii jednego modułu, drugi musi spełniać rolę pierwszego.</p> <p>B) Dostępny poprzez sieć ETHERNET 1Gb z konsoli tekstowej i protokół SSH. Zarządzanie musi być w postaci 2 szt. portów RJ45, po jednym na każdym z modułów.</p> <p>C) Zdalne zarządzanie pracą Serwerów BLADE umieszczonych wewnątrz Obudowy BLADE, w tym włączanie, wyłączanie, dostęp do konsoli serwerów w trybie tekstowym oraz graficznym, dostęp do sesji BIOS oraz podłączanie lokalnych fizycznych lub wirtualnych napędów CD/USB do serwerów.</p> <p>D) Zarządzanie Przełącznikami BLADE umieszczonymi wewnątrz Obudowy jeśli Przełączniki te są zarządzane.</p> <p>E) Monitorowanie parametrów pracy (m.in. temperatura, pobór prądu) elementów Obudowy BLADE.</p>
OB 8	<p>W każdej Obudowie BLADE musi znajdować się:</p> <p>A) 1 pary (2 szt.) lub więcej par składających się z oddzielnych Przełączników BLADE ETHERNET 10GB do realizowania co najmniej dwóch podwójnych ścieżek transmisji pakietowej.</p> <p>B) 1 para (2 szt.) lub więcej par składających się oddzielnych Przełączników</p>

	<p>BLADE FC 8G lub SAS 6G do realizacji podwójnej ścieżki transmisji blokowej.</p> <p>C) łącznie Obudowa musi być wyposażona w 4 szt. lub więcej przełączników. Zamawiający nie dopuszcza zainstalowania urządzeń pasywnych zamiast przełączników.</p>
OB 9	<p>Każdy z Przełączników BLADE ETHERNET 10Gb (Przełączniki muszą być identyczne) musi spełniać następujące wymagania.</p> <p>A) Wymagane Porty wewnętrzne:</p> <ul style="list-style-type: none"> <li>i Ilość portów musi być równa lub większa niż sumaryczna ilość Wymaganych Portów ETHERNET 10Gb we wszystkich zaoferowanych Serwerach BLADE umieszczonych w pojedynczej, zaoferowanej Obudowie BLADE.</li> </ul> <p>B) Wymagane Porty zewnętrzne:</p> <ul style="list-style-type: none"> <li>i Taka ilość portów zewnętrznych, aby na każdy zaoferowany Serwer BLADE przypadał co najmniej jeden port zewnętrzny ETHERNET 10Gb.</li> <li>ii standard portów zewnętrznych: <ul style="list-style-type: none"> <li>• co najmniej 4 porty aktywne w standardzie ETHERNET 1Gb SX,</li> <li>• co najmniej 2 porty aktywne w standardzie ETHERNET 10Gb SR.</li> </ul> </li> <li>iii Do pozostałych zaoferowanych portów należy dołączyć komplet kabli ETHERNET 10Gb DAC SFP+ o długości co najmniej 1m do podłączenia z pozostałą infrastrukturą ETHERNET.</li> </ul>
OB 10	<p>Każdy z Przełączników BLADE FC 8Gb (Przełączniki muszą być identyczne) musi spełniać następujące wymagania:</p> <p>A) Wymagane Porty wewnętrzne:</p> <ul style="list-style-type: none"> <li>i Ilość portów musi być równa lub większa niż sumaryczna ilość Wymaganych Portów 8Gb FC we wszystkich zaoferowanych Serwerach BLADE.</li> </ul> <p>Ilość portów wewnętrznych musi umożliwiać spełnienie warunku opisanego w punkcie OB 4.</p> <p>B) Wymagane Porty zewnętrzne:</p> <ul style="list-style-type: none"> <li>i Taka ilość portów zewnętrznych aby na każdy zaoferowany Serwer BLADE przypadał co najmniej jeden port zewnętrzny FC 8Gb.</li> <li>ii Wszystkie porty muszą być portami aktywnymi, gotowymi do połączeń kablowych.</li> </ul>

## 11.2.2 Serwer Blade

Serwer Blade	
Parametr	Charakterystyka (wymagania minimalne)
SBL 1	<p>Zamawiający wymaga takiej ilości serwerów aby:</p> <ul style="list-style-type: none"> <li>A) Suma mocy obliczeniowej wszystkich serwerów była równa 4,7 TFLOPS lub większa.</li> <li>B) Ilość serwerów zainstalowanych w każdej zaoferowanej obudowie BLADE była identyczna.</li> <li>C) Wszystkie serwery muszą być identyczne i każdy musi spełniać warunki opisane niżej.</li> </ul>
SBL 2	<ul style="list-style-type: none"> <li>A) Wszystkie procesory Serwerów obliczeniowych muszą być identyczne.</li> <li>B) Procesory muszą być typu x86, wykonywać instrukcje 64 bitowe oraz zawierać na sobie kontroler pamięci RAM.</li> </ul>
SBL 3	<ul style="list-style-type: none"> <li>A) Serwery muszą posiadać 256 GB lub więcej pamięci RAM.</li> <li>B) Wszystkie moduły pamięci RAM wszystkich serwerów muszą być identycznie między sobą.</li> <li>C) Połowa szczelin na pamięci RAM w każdym serwerze musi zostać nieobsadzona, gotowa do dalszej rozbudowy.</li> <li>D) Każdy serwer musi być gotowy do obsadzenia 512 GB lub więcej pamięci RAM poprzez wymianę modułów pamięci RAM pomiędzy serwerami.</li> </ul>
SBL 4	<p>Zamawiający wymaga by każdy serwer posiadał niżej wyspecyfikowane porty. Zamawiający nie dopuszcza by jakiegolwiek typ portu był przeznaczony do użycia w dwu lub więcej wymaganych standardach.</p> <ul style="list-style-type: none"> <li>A) standard: Lokalne SAS 6G <ul style="list-style-type: none"> <li>i 1 pary (2 szt.) portów lub więcej par portów dokładnie SAS 6G.</li> <li>ii Wszystkie wymagane Porty lokalne muszą być aktywne i bezpośrednio połączone z Zasobem dyskowym systemu SD-S.</li> </ul> </li> <li>B) standard: ETHERNET 10Gb <ul style="list-style-type: none"> <li>i 2 pary (4 szt.) portów lub więcej par portów ETHERNET 10Gb.</li> <li>ii Wszystkie Wymagane Porty muszą być aktywne i bezpośrednio połączone z wymaganymi Przełącznikami BLADE ETHERNET 10Gb.</li> <li>iii Sposób połączenia musi być taki, że awaria dowolnego, jednego portu ETHERNET 10G ALBO dowolnego jednego Przełącznika BLADE ETHERNET 10Gb nie przerywa transmisji danych serwera.</li> </ul> </li> <li>C) Standard: FC 8Gb <ul style="list-style-type: none"> <li>i 1 para (2 szt.) portów lub więcej par FC 8G.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>ii Wszystkie Wymagane Porty muszą być aktywne i bezpośrednio połączone z wymaganymi Przełącznikami BLADE FC.</li> <li>iii Sposób połączenia musi być taki, że awaria dowolnego, jednego portu FC 8Gb ALBO dowolnego jednego Przełącznika BLADE FC nie przerywa transmisji danych serwera.</li> </ul> <p>D) Standard: USB / SD</p> <ul style="list-style-type: none"> <li>i 1 szt. portu lub więcej pracującego w standardzie USB lub SD.</li> <li>ii Dostępny tylko po wyciągnięciu Serwera BLADE z zatoki w Obudowie BLADE.</li> </ul>
SBL 5	Cały dostarczony sprzęt musi poprawnie pracować pod kontrolą następujących systemów operacyjnych: VMWare vSphere 4.x, Red Hat Enterprise Linux 5.x, Red Hat Enterprise Linux 6.x, MS Windows Server 2008 R2 x.

### 11.2.3 Zasób dyskowy systemowy (ZD-S)

Zasób dyskowy systemowy (ZD-S)	
Parametr	Charakterystyka (wymagania minimalne)
ZDS 1	Zamawiający wymaga dostarczenia co najmniej jednego Zasobu Dyskowego ZD-S do każdego z zaoferowanych Serwerów Blade. Wszystkie Zasoby dyskowe ZD-S muszą być identyczne i spełniać warunki opisane poniżej:
ZDS 2	<p>Każdy oferowany Zasób dyskowy musi udostępniać co najmniej 600 GB przestrzeni dyskowej w postaci co najmniej 2 szt. identycznych dysków twardych o parametrach:</p> <ul style="list-style-type: none"> <li>A) Prędkość obrotowa 15.000 [RPM] o przepustowości minimum 6Gbit/s lub więcej z minimalnymi transferami 100 MB/s dla sekwencyjnego odczytu oraz 80 MB/s zapisu sekwencyjnego ALBO w technologii SSD z minimalnymi transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</li> <li>B) Wyposażony w 1 parę (2 szt.) portów SAS 6G / FC 8G. Awaria jednego portu z pary nie przerywa dostępu do danych znajdujących się na dysku.</li> </ul> <p>Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują</p>
ZDS 3	<p>Udostępnianie przestrzeni dyskowej musi odbywać się przy wykorzystaniu:</p> <ul style="list-style-type: none"> <li>A) Co najmniej 1 sztuki kontrolera wyposażonego w co najmniej 1 parę (2szt.) portów SAS 6G / FC 8G.</li> <li>B) Każdy z kontrolerów wyposażony w co najmniej 1 GB pamięci podręcznej, buforującej zapisy i odczyty. Pamięć nieulotna dostępna jednocześnie dla wszystkich zainstalowanych dysków twardych.</li> </ul>

ZDS 4	<p>Każdy Zasób dyskowy musi być zasilany i chłodzony poprzez systemy zasilania i chłodzenia opisane poniżej:</p> <p>A) Nadmiarowy, odporny na awarię 1 szt. zasilacza albo 1 szt. wiatraka system zasilania i chłodzenia.</p> <p>B) Wymienny z zewnątrz, podczas pracy, bez konieczności przerywania zadań wykonywanych przez Zasób dyskowy.</p>
-------	--

#### 11.2.4 Zasób Dyskowy Aplikacji (ZD-A)

Zasób Dyskowy Aplikacji (ZD-A)	
Parametr	Charakterystyka (wymagania minimalne)
ZD-A 1	<p>A) Zamawiający wymaga dostarczenia co najmniej jednego Zasobu dyskowego ZD-A do każdej z dostarczanych obudów BLADE.</p> <p>B) Zamawiający nie dopuszcza rozwiązań opartych o wirtualizator zasobów dyskowych, gdzie kilka urządzeń fizycznych posiadających niezależne porty do transmisji danych oraz posiadające niezależną pamięć buforującą Cache maskowane są przez kontroler bądź kontrolery z zainstalowanym oprogramowaniem wirtualizującym zasoby dyskowe.</p> <p>C) Wszystkie Zasoby dyskowe ZD-A muszą być identyczne i spełniać warunki opisane poniżej:</p>
ZD-A 2	<p>Każdy oferowany Zasób dyskowy musi udostępniać dwa rodzaje pojemności:</p> <p>Pojemność dyskowa dla danych produkcyjnych o sumarycznej wielkości 21,6 TB lub więcej w postaci 36 szt. lub więcej identycznych dysków twardych o parametrach:</p> <p>A) Prędkość obrotowa 15.000 [RPM] o przepustowości minimum 6Gbit/s lub więcej z minimalnymi transferami 100 MB/s dla sekwencyjnego odczytu oraz 80 MB/s zapisu sekwencyjnego ALBO w technologii SSD z minimalnymi transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</p> <p>B) Wyposażony w 1 parę (2 szt.) portów SAS 6G / FC 8G. Awaria jednego portu z pary nie przerywa dostępu do danych znajdujących się na dysku.</p> <p>C) Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują.</p> <p>D) Pojemność dyskowa dla danych archiwizacji o sumarycznej wielkości 24 TB lub więcej w postaci co 12 szt. lub więcej identycznych dysków twardych o parametrach</p> <p>E) Prędkość obrotowa 7.200 [RPM] o przepustowości minimum 6Gbit/s lub więcej z minimalnymi transferami 100 MB/s dla sekwencyjnego odczytu</p>

	<p>oraz 80 MB/s zapisu sekwencyjnego ALBO w technologii SSD z minimalnymi transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</p> <p>F) Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują.</p> <p>G) Musi istnieć możliwość rozbudowy Zasobu Dyskowego do co najmniej 200 Dysków Twardych w celu powiększenia przez Zamawiającego dostępnej pojemności dyskowej dla danych produkcyjnych ALBO pojemności dyskowej dla danych archiwizacji. Zamawiający dopuszcza rozbudowę Zasobu Dyskowego jedynie poprzez dołączenie dodatkowych półek dyskowych do zaoferowanego Zasobu Dyskowego. Zaoferowany Zasób dyskowy musi posiadać komplet licencji pozwalających na obsługę co najmniej 200 dysków twardych dowolnej wielkości.</p>
ZD-A 3	<p>Każdy oferowany Zasób dyskowy ZD-A musi zostać podłączony do oferowanych Przełączników BLADE FC 8Gb w sposób zapewniający spełnienie wymagań:</p> <p>A) Każdy port zasobu dyskowego ZD-A musi być w standardzie co najmniej 8Gb FC zgodny z oferowanymi portami przełączników BLADE FC 8Gb.</p> <p>B) Zasób dyskowy ZD-A musi być podłączony do wszystkich zaoferowanych przełączników BLADE FC 8Gb.</p> <p>C) Zasób dyskowy ZD-A musi być wyposażony w ilość portów odpowiadającą ilości zaoferowanych serwerów BLADE, tak, aby możliwe było utworzenie dedykowanej, fizycznej ścieżki transmisji blokowej pomiędzy każdym z oferowanych Serwerów BLADE a Zasobem Dyskowym.</p> <p>Sposób połączenia pomiędzy wymaganymi portami Zasobu dyskowego a Przełącznikami BLADE FC 8Gb musi być kablowy, bezpośredni.</p> <p>D) W sprawnym układzie w każdej transmisji danych czy to do każdego pojedynczego serwera czy do grupy serwerów musi uczestniczyć co najmniej połowa oferowanych portów Zasobu dyskowego.</p> <p>E) Awaria dowolnego ALBO jednego Portu FC 8Gb serwera ALBO jednego Przełącznika BLADE FC 8Gb ALBO jednego urządzenia, w którym znajduje się Pamięć buforująca Cache nie może przerywać transmisji danych pomiędzy Zasobem dyskowym a dowolnym serwerem.</p> <p>F) Dla każdego z zaoferowanych Serwerów BLADE Zasób dyskowy ZD-A musi udostępniać co najmniej 2GB nieulotnej pamięci Cache lub pamięci podtrzymywanej bateryjnie, buforującej zapisy oraz odczyty.</p> <p>G) Oferowana pamięć buforująca Cache musi być rozłożona na dwa niezależne urządzenia, tak aby jakakolwiek przerwa w pracy jednego z urządzeń nie przerywała transmisji danych pomiędzy Zasobem Dyskowym a Serwerami</p>

	BLADE.
ZD-A 4	<p>Oferowany Zasób dyskowy musi posiadać funkcjonalność:</p> <ul style="list-style-type: none"> <li>A) Tworzenia jednego z wybranych poziomów RAID 0,1,0+1, 5,0+5,6 na wszystkich zaoferowanych i dostępnych dyskach twardych danego typu jednocześnie.</li> <li>B) Tworzenie globalnego dysku spare.</li> <li>C) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</li> <li>D) Dynamiczną migrację danych z dysków twardych jednego typu (np. SAS/FC) na dyski twarde innego typu (np. SATA/SSD) bez przerywania dostępu serwerów do danych znajdujących się na dyskach twardych i przy wykorzystaniu wyłącznie mechanizmów sprzętowych kontrolerów zasobu dyskowego bez uczestnictwa oferowanych serwerów(ich zasobów procesorów i pamięci RAM).</li> <li>E) Wykonywania na żądanie, przy pomocy wyłącznie mechanizmów zasobu dyskowego i bez przerywania pracy serwerów korzystających z zasobów tego systemu, 500 lub więcej kopii tych samych danych w ramach systemu dyskowego bez potrzeby rezerwowania dodatkowej przestrzeni dyskowej na potrzeby tej kopii. Jeśli wymagane są licencje na powyższą funkcjonalność, należy dostarczyć licencję bez limitu ilości danych, dla których wykonywana jest kopia.</li> <li>F) Możliwość rozbudowy Zasobu Dyskowego o funkcjonalność zdalnej replikacji danych (bez przerywania pracy systemu produkcyjnego) pomiędzy zaoferowanym Zasobem Dyskowym a każdym z zaoferowanych Zasobów Dyskowych Wariant C opisanych w dalszej części specyfikacji. Zdalna replikacja musi odbywać się przy wykorzystaniu jedynie zasobów sprzętowych Zasobu Dyskowego w trybie synchronicznym jak i asynchronicznym. Rozbudowa o opisaną funkcjonalność zdalnej replikacji musi odbyć się poprzez instalację dodatkowych licencji, bez konieczności dokupowania dodatkowych elementów sprzętowych.</li> </ul>
ZD-A 5	<p>Każde urządzenie Zasobu dyskowego musi posiadać zasilanie i chłodzenie opisane niżej:</p> <ul style="list-style-type: none"> <li>A) Nadmiarowy, odporny na awarię 1 szt. zasilacza albo 1 szt. wiatraka system zasilania i chłodzenia.</li> <li>B) Wymienny z zewnątrz, podczas pracy, bez konieczności przerywania zadań wykonywanych przez Zasób dyskowy.</li> </ul>
ZD-A 6	<ul style="list-style-type: none"> <li>A) Udostępnianie dysków serwerom oraz konfigurowanie Zasobu Dyskowego musi odbywać się wyłącznie przy pomocy programowego panelu zarządzającego dostępnego z każdego serwera i musi realizować poniższe</li> </ul>



	<p>funkcjonalności:</p> <ul style="list-style-type: none"> <li>i Każdy dysk znajdujący się w Zasobie dyskowym musi być dostępny do użycia równocześnie przez wszystkie oferowane serwery.</li> <li>ii Każdy dysk znajdujący się w Zasobie dyskowym musi być dostępny wyłącznie przez dowolny, jeden serwer a niedostępny dla pozostałych.</li> </ul> <p>B) Wszystkie czynności eksploatacyjne Zasobu dyskowego muszą być wykonywane bez przerywania transmisji danych pomiędzy Zasobem dyskowym, a serwerami.</p>
ZD-A 7	Cały dostarczony sprzęt musi poprawnie pracować pod kontrolą następujących systemów operacyjnych: VMWarevSphere 4.x, Red Hat Enterprise Linux 5.x, Red Hat Enterprise Linux 6.x, MS Windows Server 2008 R2 x.

### 11.2.5 Wymagania dodatkowe

Wymagania dodatkowe	
Wymaganie	Minimalne wymagania
WDSMP 1	W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową. Zamawiający wymaga następujących usług wdrożeniowych, realizowanych w porozumieniu z Zamawiającym:
WDSMP 2	<p>Sporządzenia Planu Realizacji Zamówienia. Dokumentacja ta musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia a w szczególności:</p> <ul style="list-style-type: none"> <li>A) procedury współpracy (m.in. sposób uzgadniania zawartości i układu formularzy elektronicznych oraz opisów usług, zakres i sposób przekazania przez Partnerów informacji niezbędnych do wdrożenia<sup>3</sup>),</li> <li>B) plan wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia,</li> <li>C) plan testów systemu uwzględniających sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności</li> <li>D) Sposób i termin odbioru w podziale na każdego z partnerów,</li> <li>E) Listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu.</li> </ul>

<sup>3</sup>Wykonawca powinien uwzględnić, że Partnerzy będą mieli prawo udostępnić informacje w takiej formie (formacie, układzie), w jakiej je już posiadają, np. udostępniają na swoich stronach podmiotowych BIP.



	<p>F) Opis przypadków, w których projekt dopuszcza niedziałanie systemu.</p> <p>G) projekt dopuszcza niedziałanie systemu.</p>
WDSMP 3	Realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą. Dokumentacja Powykonawcza powinna w szczególności zawierać numery seryjne dostarczonych urządzeń powiązane z ich fizyczną lokalizacją, listę adresów sprzętowych MAC interfejsów sieciowych (lista ta musi być dostarczona również w formie elektronicznej) oraz mapę połączeń. Wszystkie połączenia kablowe powinny być oznaczone z obu stron etykietami pozwalającymi na ich jednoznaczną identyfikację i zlokalizowanie na dostarczonej z Dokumentacją Powykonawczą mapie połączeń.
WDSMP 4	W ramach wymaganych usług wdrożeniowych Zamawiający wymaga dostarczenia wszystkich niezbędnych materiałów pomocniczych takich jak: kable ETHERNET, kable INFINIBAND, kable zasilające, organizery, trwałe etykiety itp. wymagane do uzyskania opisanych w specyfikacji funkcjonalności.
WDSMP 5	Zamawiający wymaga przeprowadzenia instruktażu stanowiskowego w zakresie obsługi dostarczonego sprzętu, w miejscu jego instalacji, w wymiarze 7 godzin dla 8 osób. Tematyka instruktażu stanowiskowego powinna obejmować wszelkie czynności niezbędne do poprawnej eksploatacji dostarczonego systemu, w tym modyfikacje topologii połączeń, wymiany komponentów sprzętowych oraz obsługę interfejsów zarządzających (zarówno poprzez konsolę graficzną jak i tekstową). Plan instruktażu stanowiskowego oraz termin jego przeprowadzenia muszą zostać uzgodnione z Zamawiającym i zaakceptowane przez Zamawiającego
WDSMP 6	Warunkiem podpisania protokołu odbioru przez Zamawiającego jest zgodność stanu faktycznego wdrożenia z Dokumentacją Powykonawczą oraz pomyślne przeprowadzenie na dostarczonym sprzęcie testów według poniższej procedury:
WDSMP 7	Okres trwania testów wynosi do 14 dni od momentu ich rozpoczęcia.
WDSMP 8	Jeżeli w ciągu okresu trwania testów wystąpi jakakolwiek nieprawidłowość w funkcjonowaniu, np. samoczynny restart lub wyłączenie któregośkolwiek z dostarczonych elementów lub zanik łączności pomiędzy dostarczonymi elementami, musi być ona usunięta przez Wykonawcę i wówczas – jeżeli tak postanowi Zamawiający – cały test zostanie powtórzony.
WDSMP 9	Tylko pomyślne zakończenie ww. testów zobowiązuje podmiot odbierający do podpisania protokołu zdawczo-odbiorczego dostarczonego sprzętu.

## 11.2.6 Urządzenia sieciowe

Routery dostępne terminujące połączenia VPN	
Wymaganie	Minimalne wymagania dotyczące routerów dostępowych
US 1	<p>W ramach przygotowanej infrastruktury zaplanowano wykorzystanie dwóch urządzeń. Są to routery wyposażone w zasoby umożliwiające zestawienie sesji BGP z publiczną strukturą Internetu. Lokalizacja CPD posiada dwa łącza internetowe od niezależnych operatorów. Każde z łączy zostanie skonfigurowane na osobnym urządzeniu. Dzięki takiemu rozwiązaniu uzyskana zostanie redundancja połączenia z Internetem w dwóch przypadkach:</p> <ul style="list-style-type: none"> <li>A) Awaria jednego urządzenia.</li> <li>B) Awaria jednego z łączy internetowych operatora.</li> </ul>
US 2	<p>Urządzenie modułowe wyposażone w minimum 4 porty 1000BaseX SFP oraz posiadające minimum 1 slot do obsadzenia modułami rozszerzeń. Porty SFP muszą być obsadzone 4 konwerterami 1000BaseT.</p>
US 3	<p><u>Architektura urządzenia:</u></p> <ul style="list-style-type: none"> <li>A) wymiana modułów w trakcie pracy (ang. hot swap),</li> <li>B) redundantne zasilacze 230V AC,</li> <li>C) obudowa do montażu w szafie 19", max. 3U (zestaw montażowy dostarczony z urządzeniem).</li> </ul>
US 4	<p><u>Minimalne parametry wydajnościowe urządzenia:</u></p> <ul style="list-style-type: none"> <li>A) co najmniej 1 GB RAM,</li> <li>B) wydajność systemu na poziomie 3Mpps z możliwością rozbudowy do min. 7 Mpps,</li> <li>C) przepustowość min. 2 Gbps z możliwością rozbudowy do min. 5Gbps.</li> </ul>
US 5	<p>Urządzenie musi zapewniać obsługę następujących rodzajów interfejsów (potencjalne moduły do obsadzenia w slotach na moduły rozszerzeń):</p> <ul style="list-style-type: none"> <li>A) Ethernet: 1 Gigabit Ethernet 1000BaseX (GBIC/SFP lub równoważny), FastEthernet 10/100BaseTX,</li> <li>B) ATM – OC-3, OC-12,</li> <li>C) PoS – OC-3, OC-12,</li> <li>D) szeregowo – E1, E3, V.35.</li> </ul>
US 6	<p><u>Funkcjonalności przełączania Ethernet:</u></p> <ul style="list-style-type: none"> <li>A) obsługa 802.1Q,</li> </ul>

	B) obsługa agregacji 802.3ad (LACP).
US 7	<p><u>Funkcjonalności przełączania MPLS:</u></p> <p>A) obsługa LDP,  B) obsługa enkapsulacji VPLS,  C) MPLS L3VPN,  D) MPLS TE,  E) obsługa co najmniej 1000 instancji VRF.</p>
US 8	<p><u>Funkcjonalności routingu IP:</u></p> <p>A) obsługa IPv4 (statyczny, RIPv2, BGP, OSPF, IS-IS),  B) obsługa IPv6 (statyczny, RIPv6, OSPFv3, BGP),  C) multicast IPv4 (IGMPv3, PIM),  D) obsługa Bidirectional Forwarding Detection (BFD),  E) obsługa NonStop Forwarding,  F) obsługa VRRP lub równoważnego protokołu,  G) obsługa Unicast Reverse Path Forwarding (uRPF).</p>
US 9	<p><u>Funkcjonalności bezpieczeństwa sieciowego:</u></p> <p>A) obsługa tuneli GRE,  B) funkcjonalność zapory ogniowej typu statefull (ang. statefull firewall),  C) obsługa IPSec.</p>
US 10	<p><u>Funkcjonalności zapewnienia jakości ruchu (QoS):</u></p> <p>A) obsługa mechanizmów QoS (klasyfikacja, kolejkovanie, oznaczanie, policing, shaping),  B) obsługa hierarchicznego QoS (H-QoS),  C) możliwość klasyfikacji ruchu w oparciu o: IP DSCP, VLAN, adresy MAC i IP, protokół,  D) dynamiczna alokacja kolejek, dostępne min. 3.000 kolejek.</p>
US 11	<p><u>Funkcjonalności związane z zarządzaniem urządzeniem:</u></p> <p>A) system operacyjny o charakterze modularnym,  B) obsługa autoryzacji administratorów za pośrednictwem RADIUS,  C) obsługa Sflow lub równoważnego (J-Flow, Net-Flow),  D) obsługa MPLS OAM (LSP ping, LSP traceroute),  E) zarządzanie przez CLI (konsola szeregową), SNMPv3, XML API.</p>

## 11.2.7 System zarządzania infrastrukturą

System zarządzania infrastrukturą	
Wymaganie	Minimalne wymagania dotyczące Systemu zarządzania infrastrukturą
SZI 1	W skład systemu zarządzania wchodzić będzie sprzęt wraz z oprogramowaniem służący do realizacji reguł polityki dostępu, zarządzania logami i raportowania. System ma umożliwiać centralizację procesów zarządzania wszystkimi funkcjonalnościami elementów realizujących funkcje bezpieczeństwa w centralnym punkcie styku WAN i lokalizacjach JST. Powinny być realizowane przynajmniej poniższe funkcjonalności:
SZI 2	System zarządzania infrastrukturą musi stanowić niezależny dedykowany pakiet oprogramowania do zarządzania urządzeniami sieciowymi dostarczonymi w ramach postępowania (przełączniki, routery, bramy VPN).
SZI 3	System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru systemu, z licencją dla co najmniej 1000 urządzeń.
SZI 4	Wymagane jest, aby aplikacja pracowała w trybie klient/serwer.
SZI 5	System musi umożliwiać zbieranie statystyk co najmniej z wykorzystaniem SNMP, RMON.
SZI 6	System musi posiadać narzędzia automatycznej identyfikacji urządzeń instalowanych w sieci.
SZI 7	System musi posiadać narzędzia graficznej prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmianą stanu urządzenia (stan portu, itp.).
SZI 8	System musi posiadać narzędzia pozwalające na graficzną prezentację topologii sieci, konfigurację i monitoring sieci VLAN, uzyskanie informacji o drodze połączenia użytkownika (user tracking).
SZI 9	System musi posiadać zcentralizowany system przeglądania zdarzeń w sieci (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy).
SZI 10	System musi pozwalać na budowanie widoków przez użytkownika.
SZI 11	System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie.
SZI 12	System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń.

SZI 13	System musi posiadać funkcje zarządzania zgodnością konfiguracji oraz funkcje zarządzania zmianami w konfiguracja urządzeń sieciowych.
SZI 14	System musi posiadać wzorce konfiguracyjne pozwalające na całkowitą lub częściową konfigurację urządzeń zgodnie z zaleceniami producenta.
SZI 15	System musi posiadać narzędzie monitoringu RMON pozwalające na analizę parametrów urządzenia, łącza, portu urządzenia.
SZI 16	System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych.
SZI 17	System musi posiadać narzędzie dla automatyzacji uaktualniania oprogramowania i zmian konfiguracyjnych w urządzeniach sieciowych.
SZI 18	System musi posiadać możliwość generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku.
SZI 19	Aplikacja musi umożliwiać obsługę funkcji RBAC (Role-based Access Control) – w tym możliwość ograniczania typów zadań, jakie administrator może wykonać, jak również do jakich urządzeń ma mieć dostęp.
SZI 20	Dodatkowo na potrzeby zarządzania urządzeniami bezpieczeństwa (bramy VPN, zapory ogniowe, systemy IPS instalowane w centralnym punkcie styku i lokalizacjach JST) należy dostarczyć dodatkową aplikację (o ile poniższe funkcjonalności nie są możliwe do uzyskania z wykorzystaniem aplikacji System zarządzania infrastrukturą opisaną wyżej) spełniającą poniższe wymagania:
SZI 21	Wymagane jest, aby aplikacja pracowała w trybie klient/serwer.
SZI 22	Aplikacja musi umożliwiać konfigurację reguł firewall'a: <ul style="list-style-type: none"> <li>A) Scentralizowana konfiguracja reguł firewall'a dla obsługiwanych urządzeń.</li> <li>B) Możliwość importowania reguł z urządzenia i pliku konfiguracyjnego.</li> <li>C) Możliwość definiowania obiektów skupiających grupy interfejsów z różnych urządzeń w celu skalowalnego nakładania polityk bezpieczeństwa.</li> <li>D) Funkcja „policy query” umożliwiająca wyświetlenie reguł spełniających określone parametry takie jak źródło, cel, interfejs, usługa.</li> </ul>
SZI 23	Aplikacja musi umożliwiać konfigurację usług IPS: <ul style="list-style-type: none"> <li>A) Aplikacja musi zapewniać obsługę zarówno modułów IPS'owych będących</li> </ul>

	<p>częścią niniejszego postępowania, jak również zapewniać obsługę innych urządzeń IPS o większych przepustowościach.</p> <p>B) Możliwość konfigurowania urządzeń do pracy w trybie inline oraz promiscuous.</p> <p>C) Możliwość konfigurowania interfejsów fizycznych, par interfejsów, par sieci VLAN.</p> <p>D) Możliwość konfigurowania sensorów wirtualnych.</p> <p>E) Możliwość konfiguracji i tuningu sygnatur IPS.</p> <p>F) Możliwość konfigurowania akcji zachodzących w momencie wykrycia zagrożenia.</p> <p>G) Możliwość konfigurowania usług detekcji anomalii w ruchu sieciowym.</p> <p>H) Możliwość zarządzania aktualizacjami sygnatur dla modułów i urządzeń IPS.</p>
SZI 24	<p>Aplikacja musi ułatwiać tworzenie połączeń VPN:</p> <p>A) Kreator konfiguracji połączeń site-to-site, hub-and-spoke, jak również full-mesh.</p> <p>B) Możliwość konfiguracji połączeń IPSec i tuneli GRE.</p> <p>C) Możliwość konfiguracji połączeń typu remote access – zarówno IPSec, jak i SSL VPN.</p> <p>D) Możliwość konfiguracji dla automatycznego przełączania awaryjnego i równoważenia obciążenia dla stacji czołowej.</p>
SZI 25	<p>Oprogramowanie musi posiadać zintegrowany moduł zarządzania zdarzeniami:</p> <p>A) Wymagane jest wsparcie dla protokołów syslog i SDEE.</p> <p>B) Podgląd zdarzeń w czasie rzeczywistym, jak również danych historycznych.</p> <p>C) Opcja „Go-to-policy” dla zdarzeń będących wynikiem reguł firewall’a i sygnatur systemu IPS.</p> <p>D) Elastyczne opcje przeszukiwania, sortowania i filtrowania zdarzeń .</p>
SZI 26	<p>Aplikacja musi zapewniać elastyczność w zakresie grupowania urządzeń i możliwość zarządzania wszystkimi urządzeniami w grupie jak pojedynczym urządzeniem.</p>
SZI 27	<p>Możliwość definiowania obiektów (np. reprezentującego adresy sieciowe, parametry połączeń VPN itd.), które mogą być wielokrotnie wykorzystywane</p>
SZI 28	<p>Możliwość przypisywania zadań do różnych administratorów w czasie wdrażania polityki z opcją śledzenia i formalną kontrolą zmian.</p>

SZI 29	Aplikacja musi umożliwiać obsługę funkcji RBAC (Role-based Access Control) – w tym możliwość ograniczania typów zadań, jakie administrator może wykonać, jak również do jakich urządzeń ma mieć dostęp.
SZI 30	Aplikacja musi zostać dostarczona w najnowszej dostępnej na rynku wersji z licencją dla co najmniej 250 urządzeń.
<b>Podsystem przełączników do rozlokowania zasobów sprzętowych</b>	
<b>Wymaganie</b>	<b>Minimalne wymagania dotyczące Systemu zarządzania infrastrukturą</b>
SZI 31	<p>Przełączniki internetowe muszą zostać ze sobą połączone za pomocą dwóch linków 1000Mb/s tworzących LAG.</p> <p>Porty łączące te przełączniki muszą być w trybie trunk (tagowanie wszystkich VLANów).</p> <p>Przełącznik zarządzania musi służyć do podłączenia wszystkich interfejsów zarządzających środowiska sieciowego (może również służyć dla innych systemów). Fizycznie ze strukturą będzie on połączony za pomocą pojedynczych portów do urządzeń zapory sieciowej. Dzięki temu będzie możliwe zarządzanie strukturą z sieci innej niż zarządzająca.</p> <p>Przełączniki strefy DMZ muszą stanowić podstawę dla realizacji segmentu serwerów webowych struktury, które muszą być dostępne z Internetu.</p> <p>Strefa zdemilitaryzowana musi być również odseparowana na niezależne urządzenia ze względu na obniżony poziom bezpieczeństwa (ograniczone otwarcie ruchu z adresacji publicznych).</p>

### **11.2.8 Bezpieczeństwo sieci WAN- Zestaw urządzeń bezpieczeństwa sieci dla Centrali.**

Z punktu widzenia łatwości zarządzania, wymaga się aby wszystkie urządzenia pełniące funkcję firewall i VPN pochodziły od jednego producenta. Dla elementów systemu bezpieczeństwa obsługujących centralny punkt sieci WAN w Urzędzie Marszałkowskim i terminujących połączenia VPN z JST, Wykonawca zapewni wszystkie poniższe funkcjonalności.

#### **11.2.8.1 Urządzenia Firewall z IPS**

<b>Urządzenia Firewall/VPN</b>	
<b>Wymaganie</b>	<b>Minimalne wymagania dotyczące Urządzeń Firewall/VPN</b>
VPN 1	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łączący dla poszczególnych lokalizacji. Integralność systemu musi być zapewniona także w

	<p>przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p>
VPN 2	<p>Rozwiązanie musi być oparte o dedykowany system operacyjny – 64 bitowy. Nie dopuszcza się rozwiązań gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim posadowione oprogramowanie firewall (jako aplikacja).</p>
VPN 3	<p>Rozwiązanie powinno posiadać funkcjonalność ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.</p>
VPN 4	<p>Rozwiązanie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.</p>
VPN 5	<p>Rozwiązanie musi pozwalać na definiowanie firewalli w trybie warstwy 3 (routed) i warstwy 2 transparentnym (w warstwie L2 OSI).</p>
VPN 6	<p>Rozwiązanie musi zapewniać mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:</p> <ul style="list-style-type: none"> <li>A) Hypertext Transfer Protocol (HTTP),</li> <li>B) File Transfer Protocol (FTP),</li> <li>C) Simple Mail Transfer Protocol (SMTP),</li> <li>D) Domain Name System (DNS),</li> <li>E) H.323,</li> <li>F) Session Initiation Protocol (SIP),</li> <li>G) Lightweight Directory Access Protocol(LDAP),</li> <li>H) Internet Control Message Protocol (ICMP),</li> <li>I) Network File System (NFS).</li> </ul>
VPN 7	<p>Rozwiązanie musi zapewniać mechanizmy pozwalające na blokowanie aplikacji tunelowanych z użyciem portu 80 w tym:</p> <ul style="list-style-type: none"> <li>A) blokowanie komunikatorów internetowych.</li> <li>B) blokowanie aplikacji typu peer-to-peer.</li> </ul>
VPN 8	<p>Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego OSPF oraz RIPv2.</p>



VPN 9	<p>Rozwiązanie musi zapewniać obsługę ruchu multicast w tym:</p> <ul style="list-style-type: none"> <li>A) Protokoły routingu multicast (PIM),</li> <li>B) IGMP,</li> <li>C) definiowanie list kontroli dostępu dla ruchu multicast.</li> </ul>
VPN 10	<p>Rozwiązanie musi zapewniać obsługę ruchu z adresacją IPv6</p> <ul style="list-style-type: none"> <li>A) pracę w sieci z adresacją IPv6,</li> <li>B) definiowanie list kontroli dostępu dla ruchu IPv6,</li> <li>C) inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń,</li> <li>D) Hop-by-Hop Options,</li> <li>E) Routing (Type 0),</li> <li>F) Fragment,</li> <li>G) Destination Options,</li> <li>H) Authentication,</li> <li>I) Encapsulating Security Payload,</li> <li>J) zarządzanie urządzeniem poprzez SSHv2, HTTPS w sieci IPv6.</li> </ul>
VPN 11	Rozwiązanie musi umożliwiać zestawienie sesji IPSec VPN.
VPN 12	Rozwiązanie musi obsługiwać IKE i IKEv2.
VPN 13	Rozwiązanie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat).
VPN 14	Rozwiązanie musi obsługiwać współpracę z serwerami certyfikatów (CA).
VPN 15	Rozwiązanie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS.
VPN 16	<p>Rozwiązanie musi spełniać pełną funkcjonalność sondy systemu IPS (Intrusion Prevention System) przy pomocy dodatkowego modułu funkcjonalnego IPS. Moduł musi posiadać co najmniej następujące funkcje, w szczególności musi:</p> <ul style="list-style-type: none"> <li>A) Umożliwiać pracę w trybie IPS (In-line).</li> <li>B) Umożliwiać identyfikację, klasyfikację i powstrzymywanie ruchu zagrażającego bezpieczeństwu organizacji w tym: <ul style="list-style-type: none"> <li>i robaki sieciowe,</li> <li>ii adware,</li> <li>iii spyware,</li> </ul> </li> </ul>

	<p>iv wirusy sieciowe, v trojany, vi nadużycia aplikacyjne.</p> <p>C) Wykrywać ataki w oparciu o sygnatury oraz o wykrywanie anomalii. D) Posiadać wbudowane co najmniej 6000 sygnatur ataków. E) Umożliwiać definicje reakcji z dokładnością do jednej sygnatury. F) Umożliwiać grupowanie sygnatur ataków. G) Umożliwiać tworzenie zdarzeń opisanych przez naruszenie kilku niezależnych sygnatur ataku. H) Umożliwiać określenie znaczenia ataku na podstawie kilku zmiennych w szczególności: znaczenia atakowanego systemu, znaczenia naruszonej sygnatury oraz prawdopodobieństwa ataku. I) Umożliwiać indywidualne (przez administratora) definiowanie poziomu zagrożenia dla sygnatury. J) Zapewniać mechanizm notyfikacji administratora o zaistniałym ataku (co najmniej przez e-mail). K) Umożliwiać zarządzanie przez linię komend, graficznie przez przeglądarkę internetową oraz powinna być dostępna dedykowana aplikacja. L) Umożliwiać zdefiniowanie co najmniej 4 wirtualnych sensorów. M) Być dostarczony z aktualizacjami sygnatur na okres 5 lat od dnia dokonania odbioru końcowego.</p>
VPN 17	Rozwiązanie musi posiadać możliwość wyeksportowania konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline .
VPN 18	Rozwiązanie powinno być zarządzane przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.
VPN 19	Urządzenie musi zapewniać wydajność 10 Gbps dla ruchu IPv4 i IPv6
VPN 20	Urządzenie musi zapewniać wydajność nie mniejszą niż 3 000 000 pakietów na sekundę
VPN 21	Urządzenie musi zapewniać wydajność 3 Gbps dla jednocześnie działających funkcjonalności firewall i IPS
VPN 22	Urządzenie musi być przygotowane dla obsługi IPS z podaną wydajnością bez konieczności doposażenia go w jakiekolwiek komponenty sprzętowe, jeżeli takowe są niezbędne, należy je uwzględnić w ofercie. W momencie dostawy i

	uruchomienia projektu wymaga się dostarczenia licencji na funkcjonalność IPS.
VPN 23	Urządzenie musi zapewniać co najmniej 2Gbps dla szyfrowania VPN algorytmami 3DES/AES.
VPN 24	Urządzenie musi pozwalać na obsługę jednocześnie 10 000 tuneli IPSec. Urządzenie musi pozwalać na obsługę jednocześnie 10 000 tuneli VPN z użyciem klienta lub w trybie clientless.
VPN 25	Urządzenie musi być przygotowane dla obsługi VPN z podaną wydajnością bez konieczności doposażenia go w jakiegokolwiek komponenty sprzętowe, jeżeli takowe są niezbędne, należy je uwzględnić w ofercie. W momencie dostawy i uruchomienia projektu wymaga się dostarczenia licencji na zestawienie 2 tuneli VPN.
VPN 26	Urządzenie musi być pozwalać na zestawienie co najmniej 125 000 nowych połączeń na sekundę.
VPN 27	Urządzenie musi zapewniać obsługę co najmniej 2 000 000 jednoczesnych połączeń/translacji NAT/PAT.
VPN 28	Urządzenie musi posiadać do najmniej 16 interfejsów Gigabit Ethernet 10/100/1000Base-T i 4 interfejsy 10Gigabit Ethernet definiowane przez SFP+ (lub inny standard np. XFP).
VPN 29	Urządzenie musi poprawnie obsługiwać ramki Jumbo (9216 bajtów).
VPN 30	Urządzenie musi poprawnie obsłużyć minimum 1000 VLANów – dla IPv4 i IPv6. Urządzenie musi umożliwiać zdefiniowanie do 250 firewalli wirtualnych (dopuszcza się realizację tej funkcji przez dokupienie przez Zamawiającego dodatkowej licencji).
VPN 31	Urządzenie musi umożliwiać grupowanie VLANów w trybie pracy jako transparent firewall (Firewall warstwy 2) – minimum 8 grup po 4 VLANy. Funkcjonalność powinna być możliwa do uruchomienia dla IPv4 i IPv6.
VPN 32	Urządzenie musi umożliwiać dostęp administracyjny do interfejsu zarządzania w oparciu o role (RBAC).
VPN 33	Urządzenie musi posiadać dedykowany interfejs zarządzający GigabitEthernet do wprowadzania zmian konfiguracyjnych w trybie Out-of-Band (OOB).
VPN 34	Urządzenie musi posiadać co najmniej 2 sloty na karty rozszerzeń.
VPN 35	Urządzenie musi posiadać co najmniej 1 port USB z możliwością obsługi systemu

	plików na kluczach USB.
VPN 36	Urządzenie musi posiadać port konsoli dla realizacji lokalnego dostępu do urządzenia, może być on realizowany przez port szeregowy lub inne rozwiązanie spełniające wskazaną funkcjonalność. Port ten powinien być portem dedykowanym tzn. nie może do tego celu być wykorzystany port wyspecyfikowany powyżej.
VPN 37	Urządzenie musi pozwalać na realizację modelu wdrożenia w wysokiej dostępności dla IPv4 i IPv6 w trybach: A) Active-Standby, B) Active-Active.
VPN 38	Urządzenie musi posiadać mechanizmy pozwalające na obsługę ruchu asymetrycznego w modelu Active-Active.
VPN 39	Urządzenie musi być zasilane prądem zmiennym 230V, należy zastosować właściwy zasilacz.
VPN 40	Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego.

#### 11.2.8.2 Urządzenia LoadBalancer/SSL Terminator

Urządzenia LoadBalancer/SSL Terminator	
Wymaganie	Minimalne wymagania dotyczące Urządzeń LoadBalancer/SSL Terminator
SSL T 1	Dedykowane urządzenie umożliwiające realizację rozdziału ruchu w oparciu o informację z warstw 4-7 modelu ISO/OSI.
SSL T 2	Obsługa inteligentnego równoważenia ruchu dla farm serwerów: A) Analiza zapytań HTTP, FTP, DNS, ICMP, SIP, RTSP, RADIUS, DP. B) Możliwość manipulacji nagłówkami http.
SSL T 3	Typ i liczba portów sieciowych – minimum 4 porty 10/100/1000 (RJ45).
SSL T 4	Wymagane parametry wydajnościowe: A) Przepustowość minimum 2 Gbps z możliwością rozszerzenia do minimum 4 Gbps bez konieczności rozbudowy sprzętu. B) Obsługa minimum 1.000.000 jednoczesnych połączeń TCP. C) Obsługa minimum 100.000 połączeń na sekundę w warstwie 4. D) Obsługa minimum 1000 wirtualnych serwerów i sieci VLAN.
SSL T 5	Możliwość wirtualizacji - dostarczone urządzenie musi obsługiwać min. 10

	wirtualnych instancji z możliwością określenia zasobów (pamięć, bufor) dla każdej instancji.
SSL T 6	Możliwość monitorowania stanu serwerów i na tej podstawie dokonywania decyzji o przełączeniu połączenia do konkretnego serwera w oparciu o: <ul style="list-style-type: none"> <li>A) Obciążenie serwerów.</li> <li>B) Dostępne pasmo.</li> <li>C) Ilość połączeń.</li> <li>D) Algorytm round-robin.</li> <li>E) Próbkowanie ruchu: ICMP, TCP/UDP, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, RADIUS, SIP, dostępny język skryptowy umożliwiający tworzenie własnych testów.</li> </ul>
SSL T 7	Mechanizmy zapewnienia dowiązania sesji (session stickiness) w oparciu o: <ul style="list-style-type: none"> <li>A) Cookie.</li> <li>B) Adresy IP.</li> <li>C) Nagłówki http.</li> </ul>
SSL T 8	Mechanizmy inspekcji protokołów warstwy L7, w szczególności inspekcji ruchu HTTP, FTP, DNS, RTSP, ICMP, SIP, LDAP.
SSL T 9	Zintegrowana funkcjonalność akceleracji sesji SSL: <ul style="list-style-type: none"> <li>A) Przepustowość dla ruchu SSL minimum 1 Gbps.</li> <li>B) Obsługa minimum 7500 SSL TPS (transactions per second).</li> <li>C) SSL v3.0, TLS v1.0.</li> <li>D) Autentykacja klientów.</li> <li>E) Obsługa protokołów HTTPS, Secure IMAP, LDAPS, NNTPS, POP3S.</li> </ul>
SSL T 10	Mechanizmy ograniczania (rate limit) ruchu do poszczególnych serwerów (wirtualnych i rzeczywistych).
SSL T 11	Obsługa kompresji danych (gzip lub równoważny).
SSL T 12	Obsługa funkcjonalności cache dla http (dostępne min. 1GB pamięci RAM przeznaczonej na cache).
SSL T 13	Możliwość tworzenia kopii ruchu TCP przekazywanego przez urządzenie.
SSL T 14	Możliwość zarządzania (konfiguracja, monitoring) przez CLI (linia komend) oraz przez graficzny interfejs użytkownika.
SSL T 15	Możliwość definicji uprawnień poszczególnych administratorów w oparciu o role

	(RBAC).
SSL T 16	Wsparcie dla trybu routera i mostu (bridge) – w tym dla różnych wirtualnych instancji możliwość konfiguracji trybów routera lub mostu niezależnie.
SSL T 17	Możliwość konfiguracji w trybie redundantnym (failover) z drugim urządzeniem.
SSL T 18	Obsługa list kontroli dostępu (ACL).
SSL T 19	Obsługa mechanizmów translacji adresów i portów (NAT/PAT).
SSL T 20	Obsługa weryfikacji adresu źródłowego (uRPF).
SSL T 21	Zasilanie prądem przemiennym 230V.
SSL T 22	Obudowa przystosowana do montażu w szafie rack 19”.

### 11.2.9 Urządzenia do optymalizacji sieci WAN

Optymalizacja połączeń sieci WAN po stronie centralnej powinna być wykonana za pomocą pary urządzeń zapewniających redundancję. Do zarządzania i monitorowania parametrów związanych z optymalizacją sieci WAN należy zastosować dedykowane urządzenie.

#### 11.2.9.1 Urządzenia do optymalizacji sieci WAN po stronie centralnej

Urządzenia do Optymalizacji Sieci WAN po stronie centralnej	
Wymaganie	Minimalne wymagania dotyczące Urządzeń Optymalizacji Sieci WAN po stronie centralnej
OSW 1	<p>Urządzenie powinno umożliwiać akcelerację ruchu sieciowego TCP wykorzystując co najmniej następujące mechanizmy:</p> <ul style="list-style-type: none"> <li>a. Bezstratną kompresję danych</li> <li>b. Cache’owanie danych w warstwie transportowej (niezależne od typu aplikacji)</li> <li>c. Manipulację parametrami protokołu TCP</li> </ul>
OSW 2	<p>Urządzenie powinno umożliwiać optymalizację co najmniej następujących protokołów aplikacyjnych, przy czym przez optymalizację rozumie się ingerowanie w warstwę aplikacyjną protokołu w celu poprawy jego działania:</p> <ul style="list-style-type: none"> <li>a. CIFS/SMBv1/SMBv2</li> <li>b. MAPI oraz eMAPI</li> <li>c. HTTP</li> <li>d. NFS</li> </ul>

	e. Citrix ICA
OSW 3	Urządzenie powinno umożliwiać licencyjną rozbudowę o możliwość optymalizacji przesyłania danych wideo poprzez Microsoft Windows Media Technologies z wykorzystaniem protokołu RTSP.
OSW 4	Urządzenie musi umożliwiać rozszyfrowywanie i akcelerację ruchu sieciowego zaszyfrowanego przy pomocy protokołu SSL/TLS z zachowaniem natywnych mechanizmów szyfrowania.
OSW 5	Urządzenie musi posiadać co najmniej 24GB RAM.
OSW 6	Urządzenie musi posiadać co najmniej 5 dysków pracujące w konfiguracji RAID-5 oferującej co najmniej 2TB użytecznej przestrzeni dyskowej.
OSW 7	Urządzenie musi posiadać co najmniej dwa zasilacze prądu zmiennego 230V z możliwością wymiany uszkodzonego zasilacza bez przerywania ciągłości pracy urządzenia.
OSW 8	Urządzenie powinno móc zostać zainstalowane w szafie teleinformatycznej 19" o głębokości 80cm.
OSW 9	Urządzenie powinno posiadać metalową obudowę wysokości nie większej niż 3RU.
OSW 10	Urządzenie musi posiadać wymienne wentylatory z możliwością wymiany uszkodzonego wentylatora bez przerywania ciągłości pracy urządzenia.
OSW 11	Urządzenie musi posiadać co najmniej 2 porty typu 1 Gigabit Ethernet zgodnych z 1000BASE-T.
OSW 12	Urządzenie powinno posiadać port konsolowy.
OSW 13	Urządzenie powinno akcelerować co najmniej 16.000 równoczesnych połączeń TCP.
OSW 14	Urządzenie powinno umożliwiać przechwytywanie ruchu co najmniej przy pomocy następujących mechanizmów <ul style="list-style-type: none"> <li>a. Przekierowanie przy pomocy protokołu WCCPv2</li> <li>b. Poprzez wstawienie w ścieżkę ruchu</li> </ul>
<b>Wymaganie</b>	<b>Minimalne wymagania dotyczące LoadBalancera do Optymalizacji Sieci WAN po stronie centralnej</b>
OSW 15	Urządzenie powinno umożliwiać organizację akceleratorów po stronie centralnej w pulę i klastry w celu zapewnienia wysokiej dostępności oraz zapewnienia skalowalności rozwiązania po stronie centralnej do co najmniej 8 akceleratorów.

OSW 16	<p>Urządzenie powinno umożliwiać realizowanie zaawansowanych polityk dystrybucji akcelerowanego ruchu na podstawie co najmniej następujących informacji:</p> <ol style="list-style-type: none"> <li>Rodzaj aplikacji</li> <li>Źródłowy adres IP</li> <li>Bieżące obciążenie akceleratorów w klastrze</li> </ol>
OSW 17	<p>Urządzenie powinno posiadać co najmniej 12 portów typu 1 Gigabit Ethernet zgodnych z 100BASE-T.</p>
OSW 18	<p>Urządzenie może mieć jedną z następujących form:</p> <ol style="list-style-type: none"> <li>dedykowane urządzenie z możliwością montażu w szafie rack 19" o głębokości nie większej niż 80cm o wysokości nie większej niż 3 RU.</li> <li>dedykowanego modułu instalowanego wewnątrz urządzeń opisanych jako „Optymalizacja sieci WAN po stronie centralnej”</li> </ol>
OSW 19	<p>Urządzenie powinno umożliwiać przechwytywanie ruchu co najmniej przy pomocy jednego z następujących mechanizmów</p> <ol style="list-style-type: none"> <li>Przekierowanie przy pomocy protokołu WCCPv2</li> <li>Poprzez wstawienie w ścieżkę ruchu</li> </ol>

#### 11.2.9.2 Urządzenie do Zarządzania Optymalizacją sieci WAN po stronie centralnej

Urządzenie do Zarządzania Optymalizacją sieci WAN po stronie centralnej	
Wymaganie	Minimalne wymagania dotyczące Urządzenia do Zarządzania Optymalizacją sieci WAN po stronie centralnej
OSW-Z 1	<p>Urządzenie powinno umożliwiać akcelerację ruchu sieciowego TCP w kierunku od klienta do serwera oraz od serwera do klienta wykorzystując co najmniej następujące mechanizmy:</p> <ol style="list-style-type: none"> <li>Bezstratną kompresję danych</li> <li>Cache'owanie danych w warstwie transportowej (niezależne od typu aplikacji)</li> <li>Manipulację parametrami protokołu TCP</li> </ol>
OSW-Z 2	<p>2. Urządzenie powinno umożliwiać optymalizację co najmniej następujących protokołów aplikacyjnych, przy czym przez optymalizację rozumie się ingerowanie w warstwę aplikacyjną protokołu w celu poprawy jego działania:</p> <ol style="list-style-type: none"> <li>CIFS/SMBv1/SMBv2</li> <li>MAPI oraz eMAPI</li> </ol>



	<p>c. HTTP</p> <p>d. NFS</p> <p>e. Citrix ICA</p>
OSW-Z 3	Urządzenie powinno umożliwiać licencyjną rozbudowę o możliwość optymalizacji przesyłania danych wideo poprzez Microsoft Windows Media Technologies z wykorzystaniem protokołu RTSP.
OSW-Z 4	Urządzenie musi umożliwiać rozszyfrowywanie i akcelerację ruchu sieciowego zaszyfrowanego przy pomocy protokołu SSL/TLS z zachowaniem natywnych mechanizmów szyfrowania.
OSW-Z 5	Urządzenie powinno wykonywać akcelerację i optymalizację w sposób transparentny z zachowaniem oryginalnego połączenia TCP.
OSW-Z 6	Urządzenie musi posiadać co najmniej 16GB RAM.
OSW-Z 7	Urządzenie musi posiadać co najmniej 2 dyski pracujące w konfiguracji RAID-1 oferującej co najmniej 600GB użytecznej przestrzeni dyskowej na potrzeby mechanizmów akceleracji i optymalizacji.
OSW-Z 8	Urządzenie powinno umożliwiać licencyjną rozbudowę o możliwość uruchomienia do 6 maszyn wirtualnych.
OSW-Z 9	Urządzenie musi posiadać co najmniej jeden zasilacz prądu zmiennego 230V z możliwością rozbudowy o dodatkowy zasilacz zapasowy.
OSW-Z 10	Urządzenie powinno móc zostać zainstalowane w szafie teleinformatycznej 19" o głębokości nie większej niż 80cm.
OSW-Z 11	Urządzenie powinno posiadać metalową obudowę wysokości nie większej niż 3RU.
OSW-Z 12	Urządzenie musi posiadać wymienne wentylatory z możliwością wymiany uszkodzonego wentylatora bez przerywania ciągłości pracy urządzenia.
OSW-Z 13	Urządzenie musi posiadać co najmniej 2 porty typu 1 Gigabit Ethernet zgodnych z 1000BASE-T z możliwością opcjonalnej rozbudowy przy pomocy modułu do 10 portów typu 1 Gigabit Ethernet typu 1000BASE-T.
OSW-Z 14	Urządzenie powinno posiadać port konsolowy.
OSW-Z 15	Urządzenie powinno umożliwiać zdalne zarządzanie z linii poleceń poprzez szyfrowane połączenie SSH.
OSW-Z 16	Urządzenie powinno akcelerować co najmniej 2.500 równoczesnych połączeń TCP.

OSW-Z 17	Urządzenie powinno umożliwiać przechwytywanie ruchu co najmniej przy pomocy następujących mechanizmów a. Przekierowanie przy pomocy protokołu WCCPv2 b. Poprzez wstawienie w ścieżkę ruchu
OSW-Z 18	Urządzenie powinno umożliwiać zbieranie statystyk dotyczących optymalizacji i akceleracji sieci WAN, składować je historycznie oraz udostępniać je w formie interfejsu graficznego i eksportowalnych raportów.
OSW-Z 19	Urządzenie powinno umożliwiać centralne zarządzanie i konfigurowanie wszystkich urządzeń akcelerujących i optymalizujących w sieci.

### 11.2.10 System zarządzania incydentami

W skład systemu zarządzania incydentami wchodzi podsystem do wykrywania incydentów na bazie ruchu sieciowego z urządzeń oraz podsystem do kontroli poprawnej pracy na aplikacjach.

System zarządzania incydentami	
Wymaganie	Minimalne wymagania dotyczące systemu zarządzania incydentami
SZ IN 1	System zarządzania bezpieczeństwem musi utrzymywać centralne repozytorium logów pobieranych z innych urządzeń i systemów oraz realizować funkcje Security Information and Event Management (SIEM).
SZ IN 2	Moduł Systemu musi pobierać logi z wielu różnych elementów systemu informatycznego, poddawać je korelacji i na tej podstawie przedstawiać administratorom wiarygodne informacje na temat stanu bezpieczeństwa i wykrytych incydentów.
SZ IN 3	System zarządzania musi być dostarczony jako jedno, gotowe do użycia urządzenie Appliance. Nie jest dopuszczalne oprogramowanie instalowane na sprzęcie ogólnego przeznaczenia.
SZ IN 4	Urządzenie Appliance musi posiadać minimum 8 GB pamięci RAM oraz dysk o pojemności co najmniej 300 GB z możliwością dołączenia zewnętrznej macierzy.
SZ IN 5	Urządzenie Appliance musi posiadać wydajność co najmniej 1200 zdarzeń na sekundę oraz obsługiwać co najmniej 600 źródeł danych.
SZ IN 6	Urządzenie Appliance musi działać na bazie dostrojonego przez producenta systemu operacyjnego.
SZ IN 7	Urządzenie Appliance musi umożliwiać integrację z zewnętrznymi repozytoriami danych, co najmniej NAS.

SZ IN 8	Wszystkie funkcje systemu muszą być dostępne w ramach jednego urządzenia Appliance.
SZ IN 9	Obsługa incydentów bezpieczeństwa musi odbywać się na podstawie wielu źródeł informacji, nie mniej niż: <ul style="list-style-type: none"> <li>A) zdarzenia i logi z systemów zabezpieczeń (firewall, VPN, IPS, AV, itd.), systemów operacyjnych oraz aplikacji i baz danych,</li> <li>B) informacje na temat stanu systemów i ich słabości bezpieczeństwa odczytywane za pomocą skanerów Tenable Nessus, nCircle Configuration Compliance Manager i Qualys QualysGuard, Rapid7 Nexpose.</li> </ul>
SZ IN 10	Urządzenie musi umożliwiać pobieranie logów z innych systemów za pomocą wielu metod, co najmniej syslog, syslog NG, pliki przez ftp/sftp, SNMP, ODBC, XML przez http, Windows event log, CheckPoint OPSEC, Cisco IDS POP/DEP/SDEE.
SZ IN 11	Urządzenie musi umożliwiać odczytywanie logów z różnych systemów operacyjnych jednocześnie.
SZ IN 12	Administratorzy bezpieczeństwa muszą mieć do dyspozycji dedykowaną, graficzną konsolę narzędzia, uruchamianą z wykorzystaniem standardowej przeglądarki Web.
SZ IN 13	System zarządzania incydentami musi być wyposażony oprócz urządzenia typu appliance w dodatkowe oprogramowanie do pobierania z urządzenia zbiorów zdarzeń według zadanych parametrów w celu ich analizy offline. Użycie ww. oprogramowania powinno być możliwe po uwierzytelnieniu do urządzenia przez autoryzowanego administratora.
SZ IN 14	System zarządzania musi posiadać możliwość powiadamiania administratorów o zdarzeniach za pomocą co najmniej email, SNMP oraz Syslog.
SZ IN 15	System zarządzania musi umożliwiać przypisywanie zidentyfikowanych incydentów bezpieczeństwa do obsługi określonym administratorom.
SZ IN 16	System zarządzania musi umożliwiać definiowanie precyzyjnych uprawnień administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania - co najmniej , LDAP i LDAP over SSL/TLS.
SZ IN 17	System zarządzania do celów obsługi zdarzeń musi utrzymywać centralne repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw). Dla logów system musi utrzymywać wskaźniki czasu (time stamp).

SZ IN 18	System zarządzania musi składować informacje w bazie danych zaprojektowanej do tego celu przez producenta. Nie jest dopuszczalne użycie do tego celu bazy danych ogólnego przeznaczenia.
SZ IN 19	System zarządzania musi mieć możliwość wykonywania operacji backup i restore, uruchamianych z graficznej konsoli. System zarządzania musi mieć możliwość wykonywania archiwizacji informacji do zewnętrznych repozytoriów danych – nie mniej niż NAS.
SZ IN 20	System zarządzania musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone w wielu formatach - minimum PDF, HTML, CSV
SZ IN 21	System zarządzania musi posiadać co najmniej 1100 predefiniowanych raportów. W celu sprawnego przeszukiwania predefiniowanych raportów muszą być one pogrupowane - co najmniej według typu urządzeń i zdarzeń bezpieczeństwa. W systemie muszą być dostępne predefiniowane raporty na zgodność ze standardami bezpieczeństwa - minimum dla ISO 27002, PCI, Basel II, FISMA, HIPAA, SAS70 i SOX.
SZ IN 22	System zarządzania musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów - login/logoff i zmiany konfiguracji systemu.
SZ IN 23	System zarządzania musi posiadać możliwości weryfikacji poprawności swojego działania i powiadamiania administratorów o nieprawidłowościach - co najmniej za pomocą wpisu do logów systemowych oraz SNMP Trap.

---

## **12 Uzupełnienie struktury sieciowej urzędów JST**

### **12.1 Zakres rzeczowy**

Oferowane rozwiązanie musi uwzględniać następujące podstawowe założenia:

- a) Ponieważ mamy do czynienia z partnerami (JST) będącymi niezależnymi podmiotami, należy przyjąć, że każdy z nich może mieć własną politykę bezpieczeństwa, a co za tym idzie, musi mieć możliwość samodzielnego zarządzania urządzeniami sieciowymi realizującymi tę politykę.
- b) Jednocześnie zapewnienie bezpieczeństwa i zarządzanie konfiguracjami w ramach projektu PSeAP musi być realizowane centralnie.
- c) Nie ma możliwości w pełni bezpiecznego administrowania jednym urządzeniem przez dwóch administratorów, nawet zakładając, że obszary administrowania są dobrze zdefiniowane i rozłączne.

Z powyższych założeń wynika, że jedyną metodą spełnienia tych wymogów jest rozdzielenie urzędów i zarządzanie nimi rozłącznie: lokalnie i centralnie.

#### Rozwiązanie centralne

Realizacja połączeń JST z infrastrukturą sieciową SeUI w Urzędzie Marszałkowskim będzie realizowana z wykorzystaniem sieci internetowej oraz bezpiecznych kanałów VPN opartych o protokół IPSec. W celu realizacji takich połączeń założono, że w każdej z JST jest dostępne łącze internetowe o niezbędnej przepustowości ze stykiem Ethernet, do którego dołączyć będzie można bramę dla połączenia VPN. Wskazane jest przy tym, aby na potrzeby bramy VPN dostępny był publiczny adres IP. Warto zaznaczyć przy tym, że celem projektu nie jest zapewnienie bezpiecznego dostępu do Internetu dla JST – realizacja tego zadania leży w gestii każdej z JST (np. kontrola dostępu do Internetu, filtracja treści itp.), a jedynie zapewnienie bezpiecznego połączenia JST z centrum przetwarzania danych i infrastrukturą sieciową SeUI Urzędu Marszałkowskiego. Po stronie SeUI Urzędu Marszałkowskiego przewidziano urządzenia zapewniające:

- a) redundantne urządzenia zapewniające centralne terminowane połączeń IPSec VPN od JST oraz realizujące funkcje bezpieczeństwa - w tym funkcje zapory ogniowej i systemu ochrony przed włamaniami. Dedykowane firewalle VPN zapewnią odpowiednią wydajność dla tuneli IPSec. Tunele IPSec zostaną zestawione od każdego urzędu lokalnego. Zadaniem tuneli VPN będzie realizowanie komunikacji pomiędzy częścią centralną a urzędem lokalnym z zapewnieniem uwierzytelnienia, integralności i poufności przesyłanych danych.
- b) realizację redundantnych połączeń do sieci Internet – dwa urządzenia dołączone do dwóch niezależnych operatorów z realizacją sesji BGP z publiczną strukturą Internetu. Zapewni to zarówno odporność na awarię pojedynczego urządzenia, jak i awarię łącza internetowego jednego z operatorów. Wskazane jest, aby urządzenia te miały możliwość rozbudowy o dodatkowe funkcjonalności – w szczególności funkcje bezpieczeństwa (firewall, inspekcja pakietów itp.). Oprócz firewalli VPN zostaną zastosowane firewalle zabezpieczające część

---

centralną od strony Internetu. Firewalle te będą wyposażone w system zapobiegania włamaniom – IPS. W celu eliminacji zagrożeń i kontroli ruchu webowego generowanego przez pracowników należy zastosować Web Application Gateway.

- c) redundantne urządzenia zapewniające ciągłość usług (równoważenia obciążenia serwerów oraz zapewnienia stałej dostępności usług) – tzw. load balancer.

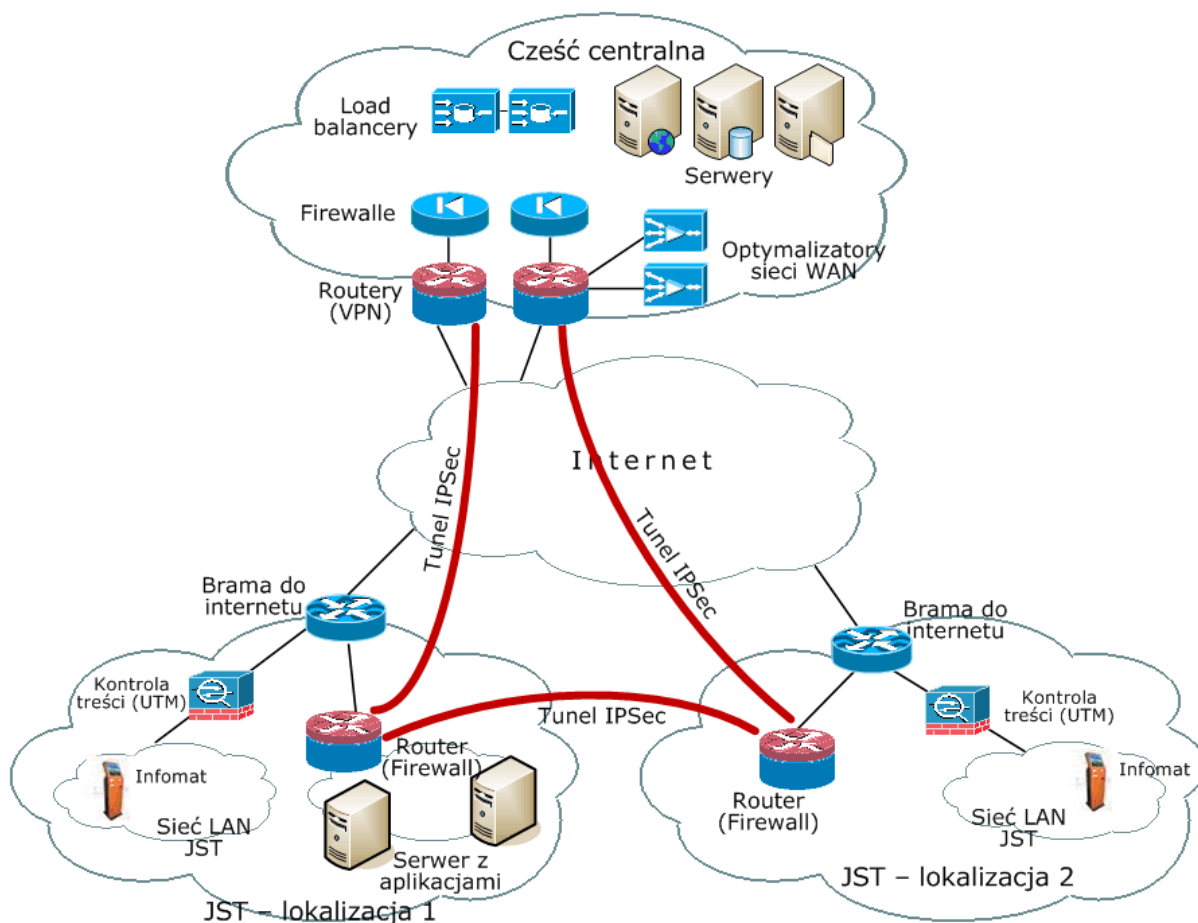
Należy zwrócić również uwagę, że obecnie realizowane rozwiązanie oparte będzie o protokół IPv4, niemniej należy przyjąć, że w niedalekiej przyszłości z uwagi na wyczerpywanie się dostępnych pól adresów IPv4 sieć ta będzie musiała migrować do protokołu IPv6 (przy czym dotyczy to części połączeniowej, jak również usługowej – czyli realizacji dostępności usług dla Usługobiorców po IPv6). Z tego powodu należy zwracać szczególną uwagę, aby urządzenia sieciowe obsługiwały zarówno protokół IPv4, jak i IPv6.

#### Rozwiązanie lokalne

Infrastruktura w urzędzie lokalnym zostanie rozszerzona o podsieć z serwerem PSeAP na którym zostaną umieszczone aplikacje dostarczane w ramach projektu PSeAP. Podsieć ta będzie zabezpieczona przez firewall. Firewall może zawierać system IPS, który wzmacnia bezpieczeństwo tej podsieci. Istniejący w urzędzie router z dwoma portami Ethernet umożliwi rozdzielanie istniejącej podsieci na część istniejącą obecnie i nową. Takie rozwiązanie umożliwi realizację bez wykonywania zmian w istniejącej sieci LAN urzędu i niezależni nową podsieć pod względem zarządzania. Dla potrzeb realizacji ochrony antywirusowej i filtrowania dostępu do nieodpowiednich treści w sieci www należy zastosować rozwiązanie klasy UTM, zapewniające jednocześnie funkcję firewall. W celu uniknięcia modyfikacji istniejących struktur logicznych takie rozwiązanie najlepiej będzie wdrożyć w trybie transparentnym (L2) pomiędzy siecią LAN a routerem. Jednocześnie ochroną realizowaną przez UTM będzie objęty informat wpięty do istniejącej sieci LAN danego urzędu. W zależności od potrzeb, to samo rozwiązanie UTM będzie mogło być również wykorzystane do ochrony antywirusowej podsieci serwerowej. Oznacza to, że dla każdej lokalizacji JST instalowany będzie zestaw co najmniej dwóch urządzeń, umożliwiający rozdzielenie administrowania pomiędzy administratora centralnego realizującego politykę bezpieczeństwa PSeAP a administratora lokalnego, realizującego politykę bezpieczeństwa JST.

W przypadku JST posiadających więcej niż jedną lokalizację połączenia między budynkami (w przypadku, gdy nie jest to sieć typu LAN, np. światłowód), będą zestawiane w ramach odrębnego VPN.





**Rysunek 6 Struktura sieciowa urzędów JST- przykład dla JST o więcej niż jednej lokalizacji**

W związku z powyższym w ramach realizacji projektu PSeAP oprócz wykonania/uzupełnienia elementów pasywnych sieci w JST, należy również dokonać opracowania schematów sieci LAN oraz dostarczyć urządzenia aktywne sieci LAN (przełączniki) przy zachowaniu poniższych założeń:

### 12.1.1 Urządzenia aktywne sieci LAN

Urządzenia aktywne sieci LAN (przełączniki)	
Wymaganie	Minimalne założenia dla Urządzeń aktywnych sieci LAN
	Ogólne
UA LAN 1	Oparcie sieci LAN o standard Gigabit Ethernet.
UA LAN 2	Zapewnienie interfejsów 10/100/1000 Mb/s dla wszystkich użytkowników sieci i odpowiednich wydajności całej ścieżki przetwarzania.
UA LAN 3	Zapewnienie mechanizmów bezpieczeństwa w sieci LAN (opracowanie polityki bezpieczeństwa w tym zakresie – np. wyłączanie nieużywanych portów, wykorzystanie funkcji typu port security itp.).



UA LAN 4	Zapewnienie mechanizmów różnicowania i priorytetyzacji ruchu w sieci LAN (QoS).
UA LAN 5	Zapewnienie mechanizmów zarządzania sieciami LAN zarówno na poziomie JST, jak i ogólno-wojewódzkim.
UA LAN 6	Dostarczenie, instalacja i konfiguracja urządzeń aktywnych sieci LAN.

## **12.1.2 Przełączniki i urządzenia bezpieczeństwa**

### **12.1.2.1 Przełączniki typu A - 24 porty 10/100/1000**

<b>Wymaganie</b>	<b>Minimalne wymagania dotyczące Przełączników typu A</b>
PA LAN 1	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack.
PA LAN 2	<p><u>Wymagane parametry fizyczne:</u></p> <ul style="list-style-type: none"> <li>A) możliwość montażu w stelażu/szafie 19",</li> <li>B) wysokość maksymalna 2U,</li> <li>C) możliwość zastosowania redundantnego zasilacza (dopuszczalne rozwiązania zewnętrzne).</li> </ul>
PA LAN 3	Przełącznik musi posiadać 24 porty Gigabit Ethernet 10/100/1000 Base-T (Auto-MDIX) oraz dodatkowe 4 interfejsy Gigabit Ethernet ze stykiem definiowanym przez moduły SFP lub równoważny.
PA LAN 4	<p>Przełącznik musi umożliwiać rozbudowę (np. poprzez instalację dodatkowego modułu) o możliwość łączenia w stosy z zachowaniem następującej funkcjonalności:</p> <ul style="list-style-type: none"> <li>A) Zarządzanie stosem poprzez jeden adres IP.</li> <li>B) Do min. 4 jednostek w stosie.</li> <li>C) Magistrala stakująca o wydajności co najmniej 20Gb/s.</li> <li>D) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack link aggregation).</li> <li>E) W lokalizacjach wyposażonych w więcej niż jeden przełącznik, należy zapewnić możliwość ich połączenia w stos (należy zapewnić komplet okablowania, modułów, itp.).</li> </ul>
PA LAN 5	Matryca przełączająca o wydajności min. 80Gbps, wydajność przełączania przynajmniej 40 mpps.
PA LAN 6	Jednoczesna obsługa min. 8.000 adresów MAC, oraz 255 sieci VLAN.

PA LAN 7	Obsługa ramek jumbo o wielkości min. 9216 bajtów.
PA LAN 8	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu STP.
PA LAN 9	Obsługa min. 16 statycznych tras dla routingu IP.
PA LAN 10	Obsługa protokołów LLDP i LLDP-MED.
PA LAN 11	Przełącznik musi posiadać możliwość uruchomienia funkcjonalności serwera DHCP.
PA LAN 12	Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping.
PA LAN 13	<p>Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:</p> <ul style="list-style-type: none"> <li>A) wiele poziomów dostępu administracyjnego poprzez konsolę,</li> <li>B) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL, obsługa VLANu dla gości,</li> <li>C) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,</li> <li>D) uwierzytelnianie użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,</li> <li>E) dostęp do urządzenia przez HTTPS, SNMPv3 i SSHv2,</li> <li>F) możliwość filtrowania ruchu w oparciu o adresy MAC, IP, porty TCP/UDP,</li> <li>G) obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, voice VLAN,</li> <li>H) możliwość synchronizacji czasu zgodnie z NTP.</li> </ul>
PA LAN 14	<p>Implementacja co najmniej czterech kolejek sprzętowych QoS na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi:</p> <ul style="list-style-type: none"> <li>A) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,</li> <li>B) obsługa jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).</li> </ul>
PA LAN 15	<p><u>Wymagane opcje zarządzania:</u></p> <ul style="list-style-type: none"> <li>A) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez określony VLAN,</li> </ul>

	<p>B) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych,</p> <p>C) dedykowany port konsoli,</p> <p>D) dedykowany port Ethernet do zarządzania,</p> <p>E) min. jeden port USB umożliwiający dołączenie zewnętrznych pamięci flash.</p>
--	--

### 12.1.2.2 Przełączniki typu B 48 portów 10/100/1000

Wymaganie	Minimalne wymagania dotyczące Przełączników typu B
PB LAN 1	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19”.
PB LAN 2	<p><u>Wymagane parametry fizyczne:</u></p> <p>A) możliwość montażu w stelażu/szafie 19”,</p> <p>B) wysokość maksymalna 2U,</p> <p>C) możliwość zastosowania redundantnego zasilacza (dopuszczalne rozwiązania zewnętrzne).</p>
PB LAN 3	Przełącznik posiada 48 portów Gigabit Ethernet 10/100/1000 Base-T (Auto-MDIX) oraz dodatkowe 4 interfejsy Gigabit Ethernet ze stykiem definiowanym przez moduły SFP lub równoważny.
PB LAN 4	<p>Przełącznik musi umożliwiać rozbudowę (np. poprzez instalację dodatkowego modułu) o możliwość łączenia w stosy z zachowaniem następującej funkcjonalności:</p> <p>A) Zarządzanie stosem poprzez jeden adres IP.</p> <p>B) Do min. 4 jednostek w stosie.</p> <p>C) Magistrala stakująca o wydajności co najmniej 20Gb/s.</p> <p>D) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack link aggregation).</p> <p>E) W lokalizacjach wyposażonych w więcej niż jeden przełącznik, należy zapewnić możliwość ich połączenia w stos (należy zapewnić komplet okablowania, modułów, itp.).</p>
PB LAN 5	Matryca przełączająca o wydajności min. 130Gbps, wydajność przełączania przynajmniej 75 mpps.

PB LAN 6	Jednoczesna obsługa min. 8.000 adresów MAC, oraz 255 sieci VLAN.
PB LAN 7	Obsługa ramek jumbo o wielkości min. 9216 bajtów.
PB LAN 8	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu STP.
PB LAN 9	Obsługa min. 16 statycznych tras dla routingu IP.
PB LAN 10	Obsługa protokołów LLDP i LLDP-MED.
PB LAN 11	Przełącznik musi posiadać możliwość uruchomienia funkcjonalności serwera DHCP.
PB LAN 12	Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping.
PB LAN 13	<p>Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:</p> <ul style="list-style-type: none"> <li>A) wiele poziomów dostępu administracyjnego poprzez konsolę,</li> <li>B) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL, obsługa VLANu dla gości,</li> <li>C) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,</li> <li>D) uwierzytelnianie użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,</li> <li>E) dostęp do urządzenia przez HTTPS, SNMPv3 i SSHv2,</li> <li>F) możliwość filtrowania ruchu w oparciu o adresy MAC, IP, porty TCP/UDP,</li> <li>G) obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, voice VLAN,</li> <li>H) możliwość synchronizacji czasu zgodnie z NTP.</li> </ul>
PB LAN 14	<p>Implementacja co najmniej czterech kolejek sprzętowych QoS na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi:</p> <ul style="list-style-type: none"> <li>A) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,</li> <li>B) obsługa jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).</li> </ul>
PB LAN 15	<p>Wymagane opcje zarządzania:</p> <ul style="list-style-type: none"> <li>A) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub</li> </ul>

	<p>poprzez określony VLAN,</p> <p>B) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych.</p>
--	--

### 12.1.3 Zestawy bezpieczeństwa

#### 12.1.3.1 Zestawy bezpieczeństwa typu A

Urządzenia bezpieczeństwa typu A	
UB A	Dla lokalizacji posiadających do 25 użytkowników, Wykonawca dostarczy sprzęt posiadający wszystkie poniższe właściwości:
UB A 1	Urządzenie musi być zasilane prądem zmiennym 230V, należy zastosować właściwy zasilacz.
UB A 2	Urządzenie o wysokości nie przekraczającej 2U - musi mieć możliwość montażu w szafie Rack 19". Jeżeli uchwyty są dostępne jako akcesoria to należy uwzględnić je w ofercie i dostarczyć w Projekcie.
UB A 3	Urządzenie pełniące rolę wielousługowego routera modularnego – w tym bramy dla połączeń VPN i systemu akceleracji ruchu
UB A 4	Minimum 3 interfejsy Gigabit Ethernet 10/100/1000
UB A 5	Możliwości instalacji co najmniej: <ul style="list-style-type: none"> <li>a. 4 kart sieciowych z interfejsami</li> <li>b. 1 modułu usługowego z interfejsami (z możliwością jego wyłączenia w celu oszczędzania energii elektrycznej)</li> <li>c. 2 modułów DSP</li> </ul> albo minimum 7 modułów ogólnego przeznaczenia do dowolnego wykorzystania
UB A 6	Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartą sieciową muszą mieć możliwość obsadzenia kartami: <ul style="list-style-type: none"> <li>a. z portami szeregowymi</li> <li>b. ze zintegrowanym modemem ADSL</li> <li>c. ze zintegrowanym modemem SHDSL</li> <li>d. z interfejsem ISDN BRI (styk S/T)</li> <li>e. z dodatkowymi portami Fast i Gigabit Ethernet</li> </ul>
UB A 7	Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy

	<p>muszą mieć możliwość obsadzenia modułami:</p> <ul style="list-style-type: none"> <li>a. z serwerem przeznaczonym do instalacji aplikacji dostarczonych przez producenta, partnerów producenta lub aplikacji napisanych na potrzeby użytkownika (muszą być dostępne narzędzia developerskie oraz wsparcie producenta)</li> <li>b. analizatora sieciowego</li> <li>c. przełącznika Ethernet (funkcje L2 i L3) o liczbie portów nie mniejszej niż 24 (w tym ze wsparciem dla PoE)</li> <li>d. kontrolera sieci bezprzewodowej</li> <li>e. poczty głosowej</li> </ul>
UB A 8	<p>Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP muszą mieć możliwość obsadzenia modułami:</p> <ul style="list-style-type: none"> <li>a. O gęstości nie mniejszej niż 128 kanałów</li> <li>b. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP</li> <li>c. Posiadającymi wsparcie dla usług głosowych i wideo</li> <li>d. Obsługującymi funkcjonalność transkodowania pomiędzy różnymi typami kodeków</li> <li>f. Obsługującymi szyfrowanie transmisji głosu z wykorzystaniem SRTP</li> </ul>
UB A 9	<p>Wszystkie interfejsy routera muszą być aktywne. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne</p>
UB A 10	<p>Urządzenie musi być wyposażone w maksymalną możliwą do zainstalowania wielkość pamięci RAM – nie mniej niż 2.5GB</p>
UB A 11	<p>Urządzenie musi posiadać co najmniej 256MB pamięci flash z możliwością jej rozbudowy do co najmniej 8GB</p>
UB A 12	<p>Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych</p>
UB A 13	<p>Urządzenie musi posiadać zainstalowany sprzętowy moduł akceleracji szyfrowania spełniający następujące wymagania:</p> <ul style="list-style-type: none"> <li>a. obsługa do 1000 tuneli IPSec VPN</li> <li>b. wydajność min. 150Mbps dla ruchu IMIX i 600Mbps dla pakietów 1400-</li> </ul>

	<p>bajtowych</p> <p>c. obsługa IPsec Internet Key Exchange (IKE): RFC 2401-2410, 2411, 2451, 4306, 4718, 4869, 5996</p> <p>d. obsługa szyfrowania w oparciu o Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) Cipher-Block Chaining (CBC) i Galois/Counter Mode (GCM) (128-, 192-, 256-bitów)</p> <p>e. wsparcie dla Diffie Hellman (DH) oraz Elliptic-Curve Diffie Hellman (ECDH)</p> <p>f. wsparcie dla Elliptic Curve Digital Signature Algorithm (ECDSA) (256-bit i 384-bit) dla podpisu certyfikatów X.509</p> <p>g. wsparcie dla walidacji certyfikatów X.509 z użyciem ECDSA</p> <p>h. wsparcie dla Message Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 i 2 (SHA-1 i SHA-2) i AES-GMAC (128-, 192-, 256- bitów)</p>
UB A 14	Urządzenie musi zapewniać możliwość konfiguracji tuneli IPv4 IPsec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2) dla rozwiązań typu DMVPN (lub równoważnych)
UB A 15	Urządzenie musi zapewniać możliwość szyfrowanie ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547
UB A 16	<p>Urządzenie musi umożliwiać akcelerację ruchu sieciowego TCP w kierunku od klienta do serwera oraz od serwera do klienta wykorzystując co najmniej następujące mechanizmy:</p> <p>a. Bezstratną kompresję danych</p> <p>b. Cache'owanie danych w warstwie transportowej (niezależne od typu aplikacji)</p> <p>c. Manipulację parametrami protokołu TCP</p>
UB A 17	<p>Urządzenie musi umożliwiać optymalizację co najmniej następujących protokołów aplikacyjnych, przy czym przez optymalizację rozumie się ingerowanie w warstwę aplikacyjną protokołu w celu poprawy jego działania:</p> <p>a. CIFS/SMBv1</p> <p>b. HTTP</p>
UB A 18	Urządzenie musi umożliwiać rozszyfrowywanie i akcelerację ruchu sieciowego zaszyfrowanego przy pomocy protokołu SSL/TLS z zachowaniem natywnych mechanizmów szyfrowania
UB A 19	Urządzenie musi wykonywać akcelerację i optymalizację w sposób transparentny z zachowaniem oryginalnego połączenia TCP

UB A 20	Możliwość równoczesnej akceleracji minimum 250 połączeń
UB A 21	Router musi mieć możliwość zarządzania poprzez CLI (konsola szeregową, SSHv2) i SNMPv3
UB A 22	Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika
UB A 23	Plik konfiguracyjny urządzenia musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (do wielkości pamięci flash). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian
UB A 24	Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora
UB A 25	Urządzenie musi oferować dla pakietów o długości 64 bajtów wydajność co najmniej 350 kpps
UB A 26	Router z uruchomionymi usługami powinien zapewniać wydajność co najmniej 35Mb/s (zgodnie z danymi i zaleceniami producenta)
UB A 27	Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i Dense) oraz routing statyczny
UB A 28	Protokół BGP musi posiadać obsługę 4 bajtowych ASN
UB A 29	Musi posiadać wsparcie dla funkcjonalności Policy Based Routing
UB A 30	Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2
UB A 31	Musi posiadać wsparcie dla protokołu DVMRP
UB A 32	Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
UB A 33	Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q
UB A 34	Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
UB A 35	Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego



	wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router)
UB A 36	Musi posiadać obsługę NAT i PAT. Mechanizm NAT musi zapewniać wsparcie dla H.224/H.245
UB A 37	Musi posiadać wsparcie dla protokołów WCCP i WCCPv2 (lub równoważnych)
UB A 38	Musi posiadać obsługę wirtualnych instancji routingu (VRF)
UB A 39	Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu
UB A 40	Musi zapewniać obsługę mechanizmów kolejkowania ruchu: <ul style="list-style-type: none"> <li>e. z obsługą kolejki absolutnego priorytetu</li> <li>f. ze statyczną alokacją pasma dla typu ruchu</li> <li>g. WFQ</li> </ul>
UB A 41	Musi obsługiwać mechanizm WRED
UB A 42	Musi obsługiwać protokół RSVP
UB A 43	Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
UB A 44	Musi obsługiwać protokół GRE oraz zapewnienia mechanizm honorowania IP Precedence dla ruchu tunelowanego
UB A 45	Musi obsługiwać protokół NTP
UB A 46	Musi obsługiwać DHCP w zakresie Client, Server
UB A 47	Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika)
UB A 48	Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
UB A 49	Musi posiadać funkcjonalność stateful firewall (w trybie routed oraz transparent)
UB A 50	Urządzenie musi posiadać możliwość rozbudowy (poprzez zakup odpowiedniej licencji lub wymianę oprogramowanie bez konieczności zmian sprzętowych) o wsparcie dla: <ul style="list-style-type: none"> <li>a. MPLS (funkcje LER i LSR), MPLS Traceroute, Traffic Engineering (w tym Fast Reroute, Link i Node Protection), Multicast dla MPLS VPN</li> <li>b. systemu IPS</li> <li>c. możliwość procesowania połączeń telefonii IP (funkcja serwera</li> </ul>

	<p>zestawiającego połączenia) dla co najmniej 50 abonentów</p> <p>d. możliwość współpracy z centralnym systemem procesowania połączeń telefonii IP w celu przejęcia podstawowych funkcji telefonii do połączeń wewnętrznych oraz wyjścia na linie miejskie na czas awarii połączenia do systemu centralnego. Funkcja ta musi być w stanie obsłużyć co najmniej 50 abonentów</p> <p>e. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych – po doposażeniu w odpowiednie interfejsy i moduły DSP (ich dostarczenie nie jest częścią tego postępowania)</p> <p>f. możliwość pracy jako mostek do połączeń VoIP wielopunktowych</p> <p>g. funkcjonalność Gatekeeper'a H.323</p> <p>h. możliwość działania jako brama IP-do-IP dla połączeń głosowych i wideo realizowanych w sieci IP</p> <p>i. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia „tam i z powrotem” (roundtrip), jitter i utraty pakietów)</p>
--	--

Urządzenia kontroli treści typu A	
Wymaganie	Minimalne wymagania dotyczące Urządzeń kontroli treści (UTM) typu A
<b>UTM A</b>	<b>Dla lokalizacji posiadających do 25 użytkowników, Wykonawca dostarczy sprzęt posiadający wszystkie poniższe właściwości:</b>
UTM A 1	Rozwiązanie powinno dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
UTM A 2	System powinien dysponować co najmniej następującymi interfejsami: A) 2 porty Ethernet 10/100/1000 Base-TX B) 6 portów Ethernet 10/100 Base-TX
UTM A 3	Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
UTM A 4	W zakresie Firewall'a obsługa nie mniej niż 100 tys jednoczesnych połączeń oraz 12 tys. nowych połączeń na sekundę
UTM A 5	Przepustowość Firewall'a: nie mniej niż 120 Mbps dla pakietów 64 bajtowych
UTM A 6	Wydajność szyfrowania IPSec: nie mniej niż 140 Mbps

UTM A 7	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:</p> <ul style="list-style-type: none"> <li>A) kontrola dostępu - zapora ogniowa klasy Stateful Inspection,</li> <li>B) ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiające skanowanie wszystkich rodzajów plików, w tym zip, rar,</li> <li>C) poufność danych - IPSec VPN oraz SSL VPN,</li> <li>D) ochrona przed atakami - Intrusion Prevention System [IPS/IDS],</li> <li>E) kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM,</li> <li>F) kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP),</li> <li>G) kontrola pasma oraz ruchu [QoS, Traffic shaping],</li> <li>H) Kontrola aplikacji oraz rozpoznawanie ruchu P2P,</li> <li>I) Możliwość analizy ruchu szyfrowanego SSL'em,</li> <li>J) Ochrona przed wyciekiem poufnej informacji (DLP).</li> </ul>
UTM A 8	Aktualizacja baza sygnatur wirusów musi być zapewniona na okres min 5 lat od dnia dokonania odbioru końcowego.
UTM A 9	Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 190 Mbps
UTM A 10	Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 350 Mbps
UTM A 11	<p>W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:</p> <ul style="list-style-type: none"> <li>A) Tworzenie połączeń w topologii Site-to-site oraz Client-to-site.</li> <li>B) Dostawca musi dostarczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem.</li> <li>C) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>D) Praca w topologii Hub and Spoke oraz Mesh.</li> <li>E) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF.</li> <li>F) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.</li> </ul>
UTM A 12	Rozwiązanie powinno zapewniać obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

UTM A 13	Możliwość budowy min 10 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
UTM A 14	Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
UTM A 15	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
UTM A 16	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
UTM A 17	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
UTM A 18	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
UTM A 19	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
UTM A 20	Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
UTM A 21	Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
UTM A 22	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: <ul style="list-style-type: none"> <li>A) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>B) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>C) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> </ul>

	D) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.
UTM A 23	Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty ICSA dla funkcjonalności Firewall, IPS, Antywirus, SSL VPN
UTM A 24	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
UTM A 25	Wymaga się aby system był wyposażony w przestrzeń dla lokalnego logowania zdarzeń o pojemności min 8 GB

#### 12.1.4 Zestawy bezpieczeństwa typu B

Wymaganie	Minimalne wymagania dotyczące Urządzeń bezpieczeństwa typu B
UB B	Dla lokalizacji posiadających od 25 do 150 użytkowników (typ B), Wykonawca dostarczy sprzęt posiadający wszystkie poniższe właściwości:
UB B 1	Urządzenie musi być zasilane prądem zmiennym 230V, należy zastosować właściwy zasilacz.
UB B 2	Urządzenie o wysokości nie przekraczającej 2U -musi mieć możliwość montażu w szafie Rack 19". Jeżeli uchwyty są dostępne jako akcesoria to należy uwzględnić je w ofercie i dostarczyć w Projekcie.
UB B 3	Urządzenie pełniące rolę wielousługowego routera modularnego – w tym bramy dla połączeń VPN i systemu akceleracji ruchu
UB B 4	Minimum 3 interfejsy Gigabit Ethernet 10/100/1000
UB B 5	Możliwości instalacji co najmniej: <ul style="list-style-type: none"> <li>a. 4 kart sieciowych z interfejsami</li> <li>b. 1 modułu usługowego z interfejsami (z możliwością jego wyłączenia w celu oszczędzania energii elektrycznej)</li> <li>c. 2 modułów DSP</li> </ul> albo minimum 7 modułów ogólnego przeznaczenia do dowolnego wykorzystania
UB B 6	Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartą sieciową muszą

	<p>mieć możliwość obsadzenia kartami:</p> <ul style="list-style-type: none"> <li>a. z portami szeregowymi</li> <li>b. ze zintegrowanym modemem ADSL</li> <li>c. ze zintegrowanym modemem SHDSL</li> <li>d. z interfejsem ISDN BRI (styk S/T)</li> <li>e. z dodatkowymi portami Fast i Gigabit Ethernet</li> </ul>
UB B 7	<p>Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy muszą mieć możliwość obsadzenia modułami:</p> <ul style="list-style-type: none"> <li>a. z serwerem przeznaczonym do instalacji aplikacji dostarczonych przez producenta, partnerów producenta lub aplikacji napisanych na potrzeby użytkownika (muszą być dostępne narzędzia developerskie oraz wsparcie producenta)</li> <li>b. analizatora sieciowego</li> <li>c. przełącznika Ethernet (funkcje L2 i L3) o liczbie portów nie mniejszej niż 24 (w tym ze wsparciem dla PoE)</li> <li>d. kontrolera sieci bezprzewodowej</li> <li>e. poczty głosowej</li> </ul>
UB B 8	<p>Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP muszą mieć możliwość obsadzenia modułami:</p> <ul style="list-style-type: none"> <li>a. O gęstości nie mniejszej niż 128 kanałów</li> <li>b. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP</li> <li>c. Posiadających wsparcie dla usług głosowych i wideo</li> <li>d. Obsługującymi funkcjonalność transkodowania pomiędzy różnymi typami kodeków</li> <li>f. Obsługującymi szyfrowanie transmisji głosu z wykorzystaniem SRTP</li> </ul>
UB B 9	<p>Wszystkie interfejsy routera muszą być aktywne. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne</p>
UB B 10	<p>Urządzenie musi być wyposażone w maksymalną możliwą do zainstalowania wielkość pamięci RAM – nie mniej niż 2.5GB</p>
UB B 11	<p>Urządzenie musi posiadać co najmniej 256MB pamięci flash z możliwością jej rozbudowy do co najmniej 8GB</p>
UB B 12	<p>Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą</p>

	pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych
UB B 13	<p>Urządzenie musi posiadać zainstalowany sprzętowy moduł akceleracji szyfrowania spełniający następujące wymagania:</p> <ul style="list-style-type: none"> <li>a. obsługa do 1000 tuneli IPSec VPN</li> <li>b. wydajność min. 150Mbps dla ruchu IMIX i 600Mbps dla pakietów 1400-bajtowych</li> <li>c. obsługa IPsec Internet Key Exchange (IKE): RFC 2401-2410, 2411, 2451, 4306, 4718, 4869, 5996</li> <li>d. obsługa szyfrowania w oparciu o Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) Cipher-Block Chaining (CBC) i Galois/Counter Mode (GCM) (128-, 192-, 256-bitów)</li> <li>e. wsparcie dla Diffie Hellman (DH) oraz Elliptic-Curve Diffie Hellman (ECDH)</li> <li>f. wsparcie dla Elliptic Curve Digital Signature Algorithm (ECDSA) (256-bit i 384-bit) dla podpisu certyfikatów X.509</li> <li>g. wsparcie dla walidacji certyfikatów X.509 z użyciem ECDSA</li> <li>h. wsparcie dla Message Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 i 2 (SHA-1 i SHA-2) i AES-GMAC (128-, 192-, 256-bitów)</li> </ul>
UB B 14	Urządzenie musi zapewniać możliwość konfiguracji tuneli IPv4 IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2) dla rozwiązań typu DMVPN (lub równoważnych)
UB B 15	Urządzenie musi zapewniać możliwość szyfrowanie ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547
UB B 16	<p>Urządzenie musi umożliwiać akcelerację ruchu sieciowego TCP w kierunku od klienta do serwera oraz od serwera do klienta wykorzystując co najmniej następujące mechanizmy:</p> <ul style="list-style-type: none"> <li>a. Bezstratną kompresję danych</li> <li>b. Cache'owanie danych w warstwie transportowej (niezależne od typu aplikacji)</li> <li>c. Manipulację parametrami protokołu TCP</li> </ul>
UB B 17	Urządzenie musi umożliwiać optymalizację co najmniej następujących protokołów aplikacyjnych, przy czym przez optymalizację rozumie się ingerowanie w warstwę aplikacyjną protokołu w celu poprawy jego działania:

	a. CIFS/SMBv1 b. HTTP
UB B 18	Urządzenie musi umożliwiać rozszyfrowywanie i akcelerację ruchu sieciowego zaszyfrowanego przy pomocy protokołu SSL/TLS z zachowaniem natywnych mechanizmów szyfrowania
UB B 19	Urządzenie musi wykonywać akcelerację i optymalizację w sposób transparentny z zachowaniem oryginalnego połączenia TCP
UB B 20	Możliwość równoczesnej akceleracji minimum 250 połączeń
UB B 21	Router musi mieć możliwość zarządzania poprzez CLI (konsola szeregową, SSHv2) i SNMPv3
UB B 22	Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika
UB B 23	Plik konfiguracyjny urządzenia musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (do wielkości pamięci flash). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian
UB B 24	Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora
UB B 25	Urządzenie musi oferować dla pakietów o długości 64 bajtów wydajność co najmniej 350 kpps
UB B 26	Router z uruchomionymi usługami powinien zapewniać wydajność co najmniej 35Mb/s (zgodnie z danymi i zaleceniami producenta)
UB B 27	Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i Dense) oraz routing statyczny
UB B 28	Protokół BGP musi posiadać obsługę 4 bajtowych ASN
UB B 29	Musi posiadać wsparcie dla funkcjonalności Policy Based Routing
UB B 30	Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2
UB B 31	Musi posiadać wsparcie dla protokołu DVMRP



UB B 32	Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
UB B 33	Musi obsługiwać tzw.routing między sieciami VLAN w oparciu o trunking 802.1Q
UB B 34	Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
UB B 35	Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router)
UB B 36	Musi posiadać obsługę NAT i PAT. Mechanizm NAT musi zapewniać wsparcie dla H.224/H.245
UB B 37	Musi posiadać wsparcie dla protokołów WCCP i WCCPv2 (lub równoważnych)
UB B 38	Musi posiadać obsługę wirtualnych instancji routingu (VRF)
UB B 39	Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu
UB B 40	Musi zapewniać obsługę mechanizmów kolejkowania ruchu: <ul style="list-style-type: none"> <li>e. z obsługą kolejki absolutnego priorytetu</li> <li>f. ze statyczną alokacją pasma dla typu ruchu</li> <li>g. WFQ</li> </ul>
UB B 41	Musi obsługiwać mechanizm WRED
UB B 42	Musi obsługiwać protokół RSVP
UB B 43	Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
UB B 44	Musi obsługiwać protokół GRE oraz zapewnienia mechanizm honorowania IP Precedence dla ruchu tunelowanego
UB B 45	Musi obsługiwać protokół NTP
UB B 46	Musi obsługiwać DHCP w zakresie Client, Server
UB B 47	Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika)
UB B 48	Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
UB B 49	Musi posiadać funkcjonalność stateful firewall (w trybie routed oraz transparent)

UB B 50	<p>Urządzenie musi posiadać możliwość rozbudowy (poprzez zakup odpowiedniej licencji lub wymianę oprogramowanie bez konieczności zmian sprzętowych) o wsparcie dla:</p> <ul style="list-style-type: none"> <li>a. MPLS (funkcje LER i LSR), MPLS Traceroute, Traffic Engineering (w tym Fast Reroute, Link i Node Protection), Multicast dla MPLS VPN</li> <li>b. systemu IPS</li> <li>c. możliwość procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia) dla co najmniej 50 abonentów</li> <li>d. możliwość współpracy z centralnym systemem procesowania połączeń telefonii IP w celu przejęcia podstawowych funkcji telefonii do połączeń wewnętrznych oraz wyjścia na linie miejskie na czas awarii połączenia do systemu centralnego. Funkcja ta musi być w stanie obsłużyć co najmniej 50 abonentów</li> <li>e. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych – po doposażeniu w odpowiednie interfejsy i moduły DSP (ich dostarczenie nie jest częścią tego postępowania)</li> <li>f. możliwość pracy jako mostek do połączeń VoIP wielopunktowych</li> <li>g. funkcjonalność Gatekeeper'a H.323</li> <li>h. możliwość działania jako brama IP-do-IP dla połączeń głosowych i wideo realizowanych w sieci IP</li> <li>i. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia „tam i z powrotem” (roundtrip), jitter i utraty pakietów)</li> </ul>
---------	--

Urządzenia kontroli treści typu B	
Wymaganie	Minimalne wymagania dotyczące Urządzeń kontroli treści (UTM) typu B
<b>UTM B</b>	<b>Dla lokalizacji posiadających od 25 do 150 użytkowników, Wykonawca dostarczy sprzęt posiadający wszystkie poniższe właściwości:</b>
UTM B 1	Rozwiązanie powinno dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
UTM B 2	System musi dysponować co najmniej 8 portami Ethernet 10/100/1000 Base-TX
UTM B 3	Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
UTM B 4	Obsługa nie mniej niż 400 tys jednoczesnych połączeń oraz 3 tys. nowych połączeń

	na sekundę
UTM B 5	Przepustowość dla funkcji firewall: nie mniej niż 500 Mbps
UTM B 6	Wydajność szyfrowania IPSec: nie mniej niż 60 Mbps
UTM B 7	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:</p> <ul style="list-style-type: none"> <li>A) kontrola dostępu - zaporą ogniową klasy Stateful Inspection,</li> <li>B) ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar,</li> <li>C) poufność danych - IPSec VPN oraz SSL VPN,</li> <li>D) ochrona przed atakami - Intrusion Prevention System [IPS/IDS],</li> <li>E) kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM,</li> <li>F) kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP),</li> <li>G) kontrola pasma oraz ruchu [QoS, Traffic shaping],</li> <li>H) kontrola aplikacji oraz rozpoznawanie ruchu P2P,</li> <li>I) ochrona przed wyciekiem poufnej informacji (DLP).</li> </ul>
UTM B 8	Aktualizacja baza sygnatur wirusów musi być zapewniona na okres min 5 lat od dnia dokonania odbioru końcowego.
UTM B 9	Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 40 Mbps
UTM B 10	Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 130 Mbps
UTM B 11	<p>W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:</p> <ul style="list-style-type: none"> <li>A) Tworzenie połączeń w topologii Site-to-site oraz Client-to-site.</li> <li>B) Dostawca musi dostarczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem.</li> <li>C) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>D) Praca w topologii Hub and Spoke oraz Mesh.</li> <li>E) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF.</li> <li>F) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.</li> </ul>

UTM B 12	Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
UTM B 13	Możliwość budowy min 10 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
UTM B 14	Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
UTM B 15	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
UTM B 16	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
UTM B 17	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
UTM B 18	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
UTM B 19	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
UTM B 20	Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam, Proxy avoidance). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
UTM B 21	Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
UTM B 22	Wymaga się, aby system był wyposażony w przestrzeń dla lokalnego logowania zdarzeń o pojemności min 8 GB.

## 12.1.5 Urządzenia bezpieczeństwa typu C

Urządzenia bezpieczeństwa typu C	
Wymaganie	Minimalne wymagania dotyczące Urządzeń bezpieczeństwa typu C
UB C	Dla lokalizacji posiadających od 150 do 300 użytkowników, Wykonawca zapewni sprzęt posiadający wszystkie poniższe właściwości:
UB C 1	Urządzenie musi być zasilane prądem zmiennym 230V, należy zastosować właściwy zasilacz. Urządzenie musi mieć możliwość instalacji zasilacza redundantnego.
UB C 2	Urządzenie o wysokości nie przekraczającej 2U- musi mieć możliwość montażu w szafie Rack 19". Jeżeli uchwyty są dostępne jako akcesoria to należy uwzględnić je w ofercie i dostarczyć w Projekcie.
UB C 3	Urządzenie pełniące rolę wielousługowego routera modularnego – w tym bramy dla połączeń VPN i systemu akceleracji ruchu
UB C 4	Minimum 3 interfejsy Gigabit Ethernet 10/100/1000. Co najmniej jeden interfejs musi mieć możliwość pracy w trybie „dual-physical” z gigabitowym portem światłowodowym definiowanym przez SFP
UB C 5	Możliwości instalacji co najmniej: <ul style="list-style-type: none"> <li>a. 4 kart sieciowych z interfejsami</li> <li>b. 1 modułu usługowego z interfejsami (z możliwością jego wyłączenia w celu oszczędzania energii elektrycznej)</li> <li>c. 3 modułów DSP</li> </ul> albo minimum 8 modułów ogólnego przeznaczenia do dowolnego wykorzystania
UB C 6	Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartą sieciową muszą mieć możliwość obsadzenia kartami: <ul style="list-style-type: none"> <li>a. z portami szeregowymi</li> <li>b. ze zintegrowanym modemem ADSL</li> <li>c. ze zintegrowanym modemem SHDSL</li> <li>d. z interfejsem ISDN BRI (styk S/T)</li> <li>e. z dodatkowymi portami Fast i Gigabit Ethernet</li> </ul>
UB C 7	Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy muszą mieć możliwość obsadzenia modułami: <ul style="list-style-type: none"> <li>a. z serwerem przeznaczonym do instalacji aplikacji dostarczonych przez producenta, partnerów producenta lub aplikacji napisanych na potrzeby</li> </ul>

	<p>użytkownika (muszą być dostępne narzędzia developerskie oraz wsparcie producenta)</p> <ul style="list-style-type: none"> <li>b. analizatora sieciowego</li> <li>c. przełącznika Ethernet (funkcje L2 i L3) o liczbie portów nie mniejszej niż 50 (w tym ze wsparciem dla PoE)</li> <li>d. kontrolera sieci bezprzewodowej</li> <li>e. poczty głosowej</li> </ul>
UB C 8	<p>Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP muszą mieć możliwość obsadzenia modułami:</p> <ul style="list-style-type: none"> <li>a. O gęstości nie mniejszej niż 128 kanałów</li> <li>b. Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP</li> <li>c. Posiadającymi wsparcie dla usług głosowych i wideo</li> <li>d. Obsługującymi funkcjonalność transkodowania pomiędzy różnymi typami kodeków</li> <li>f. Obsługującymi szyfrowanie transmisji głosu z wykorzystaniem SRTP</li> </ul>
UB C 9	<p>Wszystkie interfejsy routera muszą być aktywne. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne</p>
UB C 10	<p>Urządzenie musi być wyposażone w maksymalną możliwą do zainstalowania wielkość pamięci RAM – nie mniej niż 2.5GB</p>
UB C 11	<p>Urządzenie musi posiadać co najmniej 256MB pamięci flash z możliwością jej rozbudowy do co najmniej 8GB</p>
UB C 12	<p>Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych</p>
UB C 13	<p>Urządzenie musi posiadać zainstalowany sprzętowy moduł akceleracji szyfrowania spełniający następujące wymagania:</p> <ul style="list-style-type: none"> <li>a. obsługa do 1500 tuneli IPSec VPN</li> <li>b. wydajność min. 200Mbps dla ruchu IMIX i 700Mbps dla pakietów 1400-bajtowych</li> <li>c. obsługa IPsec Internet Key Exchange (IKE): RFC 2401-2410, 2411, 2451, 4306, 4718, 4869, 5996</li> </ul>

	<p>d. obsługa szyfrowania w oparciu o Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) Cipher-Block Chaining (CBC) i Galois/Counter Mode (GCM) (128-, 192-, 256-bitów)</p> <p>e. wsparcie dla Diffie Hellman (DH) oraz Elliptic-Curve Diffie Hellman (ECDH)</p> <p>f. wsparcie dla Elliptic Curve Digital Signature Algorithm (ECDSA) (256-bit i 384-bit) dla podpisu certyfikatów X.509</p> <p>g. wsparcie dla walidacji certyfikatów X.509 z użyciem ECDSA</p> <p>h. wsparcie dla Message Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 i 2 (SHA-1 i SHA-2) i AES-GMAC (128-, 192-, 256- bitów)</p>
UB C 14	Urządzenie musi zapewniać możliwość konfiguracji tuneli IPv4 IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2) dla rozwiązań typu DMVPN (lub równoważnych)
UB C 15	Urządzenie musi zapewniać możliwość szyfrowanie ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547
UB C 16	<p>Urządzenie musi umożliwiać akcelerację ruchu sieciowego TCP w kierunku od klienta do serwera oraz od serwera do klienta wykorzystując co najmniej następujące mechanizmy:</p> <p>a. Bezstratną kompresję danych</p> <p>b. Cache'owanie danych w warstwie transportowej (niezależne od typu aplikacji)</p> <p>c. Manipulację parametrami protokołu TCP</p>
UB C 17	<p>Urządzenie musi umożliwiać optymalizację co najmniej następujących protokołów aplikacyjnych, przy czym przez optymalizację rozumie się ingerowanie w warstwę aplikacyjną protokołu w celu poprawy jego działania:</p> <p>a. CIFS/SMBv1</p> <p>b. http</p>
UB C 18	Urządzenie musi umożliwiać rozszyfrowywanie i akcelerację ruchu sieciowego zaszyfrowanego przy pomocy protokołu SSL/TLS z zachowaniem natywnych mechanizmów szyfrowania
UB C 19	Urządzenie musi wykonywać akcelerację i optymalizację w sposób transparentny z zachowaniem oryginalnego płaczenia TCP
UB C 20	Możliwość równoczesnej akceleracji minimum 250 połączeń
UB C 21	Router musi mieć możliwość zarządzania poprzez CLI (konsola szeregową, SSHv2) i

	SNMPv3
UB C 22	Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika
UB C 23	Plik konfiguracyjny urządzenia musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (do wielkości pamięci flash). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian
UB C 24	Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora
UB C 25	Urządzenie musi oferować dla pakietów o długości 64 bajtów wydajność co najmniej 450 kpps
UB C 26	Router z uruchomionymi usługami powinien zapewniać wydajność co najmniej 50Mb/s (zgodnie z danymi i zaleceniami producenta)
UB C 27	Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i Dense) oraz routing statyczny
UB C 28	Protokół BGP musi posiadać obsługę 4 bajtowych ASN
UB C 29	Musi posiadać wsparcie dla funkcjonalności Policy Based Routing
UB C 30	Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2
UB C 31	Musi posiadać wsparcie dla protokołu DVMRP
UB C 32	Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
UB C 33	Musi obsługiwać tzw.routing między sieciami VLAN w oparciu o trunking 802.1Q
UB C 34	Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
UB C 35	Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router)
UB C 36	Musi posiadać obsługę NAT i PAT. Mechanizm NAT musi zapewniać wsparcie dla



	H.224/H.245
UB C 37	Musi posiadać wsparcie dla protokołów WCCP i WCCPv2 (lub równoważnych)
UB C 38	Musi posiadać obsługę wirtualnych instancji routingu (VRF)
UB C 39	Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu
UB C 40	Musi zapewniać obsługę mechanizmów kolejkowania ruchu: <ul style="list-style-type: none"> <li>a. z obsługą kolejki absolutnego priorytetu</li> <li>b. ze statyczną alokacją pasma dla typu ruchu</li> <li>c. WFQ</li> </ul>
UB C 41	Musi obsługiwać mechanizm WRED
UB C 42	Musi obsługiwać protokół RSVP
UB C 43	Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
UB C 44	Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precedence dla ruchu tunelowanego
UB C 45	Musi obsługiwać protokół NTP
UB C 46	Musi obsługiwać DHCP w zakresie Client, Server
UB C 47	Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika)
UB C 48	Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
UB C 49	Musi posiadać funkcjonalność stateful firewall (w trybie routed oraz transparent)
UB C 50	Urządzenie musi posiadać możliwość rozbudowy (poprzez zakup odpowiedniej licencji lub wymianę oprogramowanie bez konieczności zmian sprzętowych) o wsparcie dla: <ul style="list-style-type: none"> <li>a. MPLS (funkcje LER i LSR), MPLS Traceroute, Traffic Engineering (w tym Fast Reroute, Link i Node Protection), Multicast dla MPLS VPN</li> <li>b. systemu IPS</li> <li>c. możliwość procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia) dla co najmniej 100 abonentów</li> <li>d. możliwość współpracy z centralnym systemem procesowania połączeń telefonii IP w celu przejęcia podstawowych funkcji telefonii do połączeń</li> </ul>

	<p>wewnętrznych oraz wyjścia na linie miejskie na czas awarii połączenia do systemu centralnego. Funkcja ta musi być w stanie obsłużyć co najmniej 100 abonentów</p> <p>e. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych – po doposażeniu w odpowiednie interfejsy i moduły DSP (ich dostarczenie nie jest częścią tego postępowania)</p> <p>f. możliwość pracy jako mostek do połączeń VoIP wielopunktowych</p> <p>g. funkcjonalność Gatekeeper’a H.323</p> <p>h. możliwość działania jako brama IP-do-IP dla połączeń głosowych i wideo realizowanych w sieci IP</p> <p>i. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia „tam i z powrotem” (roundtrip), jitter i utraty pakietów)</p>
--	---

Urządzenia kontroli treści typu C	
Wymaganie	Minimalne wymagania dotyczące Urządzeń kontroli treści (UTM) typu C
<b>UTM C</b>	<b>Dla lokalizacji posiadających od 150 do 300 użytkowników, Wykonawca dostarczy sprzęt posiadający wszystkie poniższe właściwości:</b>
UTM C 1	Rozwiązanie powinno dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
UTM C 2	System realizujący funkcję Firewall powinien dysponować minimum 20 interfejsami miedzianymi Ethernet 10/100/1000 pracującymi niezależnie.
UTM C 3	Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
UTM C 4	W zakresie Firewall’a obsługa nie mniej niż 2,5 milion jednoczesnych połączeń oraz 22 tys. nowych połączeń na sekundę.
UTM C 5	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:</p> <p>A) Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>B) Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.</p>

	<p>C) Poufność danych - IPSec VPN oraz SSL VPN.</p> <p>D) Ochrona przed atakami - Intrusion Prevention System [IPS/IDS].</p> <p>E) Kontrola stron Internetowych – Web Filter [WF].</p> <p>F) Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP).</p> <p>G) Kontrola pasma oraz ruchu [QoS i Traffic shaping].</p> <p>H) Kontrola aplikacji oraz rozpoznawanie ruchu P2P.</p> <p>I) Możliwość analizy ruchu szyfrowanego SSL'em.</p> <p>J) Ochrona przed wyciekami poufnej informacji (DLP).</p> <p>K) Wydajność systemu Firewall min 200Mbps dla pakietów 64 bajtowych.</p>
UTM C 6	Aktualizacja baza sygnatur wirusów musi być zapewniona na okres min 5 lat od dnia dokonania odbioru końcowego.
UTM C 7	Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 700 Mbps
UTM C 8	Wydajność ochrony przed atakami (IPS) min 950 Mbps.
UTM C 9	Wydajność szyfrowania IPSec, nie mniej niż 450 Mbps
UTM C 10	<p>W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:</p> <p>A) Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.</p> <p>B) Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem.</p> <p>C) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>D) Praca w topologii Hub and Spoke oraz Mesh.</p> <p>E) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF.</p> <p>F) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.</p>
UTM C 11	Rozwiązanie powinno zapewniać obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
UTM C 12	Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
UTM C 13	Możliwość budowy min 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
UTM C 14	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP,

	interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
UTM C 15	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
UTM C 16	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
UTM C 17	Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
UTM C 18	Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
UTM C 19	Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 55 kategorii (np. IT, Zakupy). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
UTM C 20	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
UTM C 21	Wymaga się aby dostarczony system oferował możliwość uruchomienia funkcjonalności optymalizacji ruchu WAN, korzystającą minimum z techniki byte-caching, w celu jak najlepszego wykorzystania dostępnych łącz internetowych.
UTM C 22	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: <ul style="list-style-type: none"> <li>A) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>B) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>C) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> <li>D) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory.</li> </ul>

UTM C 23	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: A) ICSA lub EAL4 – dla funkcjonalności Firewall.
UTM C 24	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
UTM C 25	Wymaga się, aby system był wyposażony w przestrzeń dla lokalnego logowania zdarzeń o pojemności min 8 GB

### 12.1.6 Urządzenia bezpieczeństwa typu D

Urządzenia bezpieczeństwa typu D	
Wymaganie	Minimalne wymagania dotyczące Urządzeń bezpieczeństwa typu D
UB D	Dla lokalizacji JST posiadających ogółem powyżej 300 użytkowników Wykonawca dostarczy sprzęt posiadający wszystkie poniższe właściwości:
UB D 1	Urządzenie musi być zasilane prądem zmiennym 230V, należy zastosować właściwy zasilacz. Urządzenie musi mieć możliwość instalacji zasilacza redundantnego.
UB D 2	Urządzenie o wysokości nie przekraczającej 2U musi mieć możliwość montażu w szafie Rack 19". Jeżeli uchwyty są dostępne jako akcesoria to należy uwzględnić je w ofercie i dostarczyć w projekcie.
UB D 3	Urządzenie pełniące rolę wielousługowego routera modularnego – w tym bramy dla połączeń VPN i systemu akceleracji ruchu
UB D 4	Minimum 3 interfejsy Gigabit Ethernet 10/100/1000. Co najmniej dwa interfejsy muszą mieć możliwość pracy w trybie „dual-physical” z gigabitowym portem światłowodowym definiowanym przez SFP
UB D 5	Możliwości instalacji co najmniej: <ul style="list-style-type: none"> <li>a. 4 kart sieciowych z interfejsami</li> <li>b. 4 modułów usługowych z interfejsami (z możliwością ich wyłączenia w celu oszczędzania energii elektrycznej)</li> <li>c. 4 modułów DSP</li> </ul> albo minimum 12 modułów ogólnego przeznaczenia do dowolnego wykorzystania



UB D 6	<p>Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartą sieciową muszą mieć możliwość obsadzenia kartami:</p> <ol style="list-style-type: none"><li>z portami szeregowymi</li><li>ze zintegrowanym modemem ADSL</li><li>ze zintegrowanym modemem SHDSL</li><li>z interfejsem ISDN BRI (styk S/T)</li><li>z dodatkowymi portami Fast i Gigabit Ethernet</li></ol>
UB D 7	<p>Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł usługowy muszą mieć możliwość obsadzenia modułami:</p> <ol style="list-style-type: none"><li>z serwerem przeznaczonym do instalacji aplikacji dostarczonych przez producenta, partnerów producenta lub aplikacji napisanych na potrzeby użytkownika (muszą być dostępne narzędzia developerskie oraz wsparcie producenta)</li><li>analizatora sieciowego</li><li>przełącznika Ethernet (funkcje L2 i L3) o liczbie portów nie mniejszej niż 50 (w tym ze wsparciem dla PoE)</li><li>kontrolera sieci bezprzewodowej</li><li>poczty głosowej</li></ol>
UB D 8	<p>Sloty urządzenia przewidziane pod rozbudowę o moduł z układami DSP muszą mieć możliwość obsadzenia modułami:</p> <ol style="list-style-type: none"><li>O gęstości nie mniejszej niż 128 kanałów</li><li>Pozwalającymi na dynamiczne alokowanie DSP do różnych zadań (obsługa interfejsów głosowych, transcoding, conferencing) z granulacją do 1 DSP</li><li>Posiadających wsparcie dla usług głosowych i wideo</li><li>Obsługującymi funkcjonalność transkodowania pomiędzy różnymi typami kodeków</li><li>Obsługującymi szyfrowanie transmisji głosu z wykorzystaniem S RTP</li></ol>
UB D 9	<p>Wszystkie interfejsy routera muszą być aktywne. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne</p>
UB D 10	<p>Urządzenie musi być wyposażone w maksymalną możliwą do zainstalowania wielkość pamięci RAM – nie mniej niż 4GB</p>
UB D 11	<p>Urządzenie musi posiadać co najmniej 256MB pamięci flash z możliwością jej rozbudowy do co najmniej 8GB</p>

UB D 12	Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych
UB D 13	<p>Urządzenie musi posiadać zainstalowany sprzętowy moduł akceleracji szyfrowania spełniający następujące wymagania:</p> <ul style="list-style-type: none"> <li>a. obsługa do 3000 tuneli IPsec VPN</li> <li>b. wydajność min. 600Mbps dla ruchu IMIX i 1200Mbps dla pakietów 1400-bajtowych</li> <li>c. obsługa IPsec Internet Key Exchange (IKE): RFC 2401-2410, 2411, 2451, 4306, 4718, 4869, 5996</li> <li>d. obsługa szyfrowania w oparciu o Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES) Cipher-Block Chaining (CBC) i Galois/Counter Mode (GCM) (128-, 192-, 256-bitów)</li> <li>e. wsparcie dla Diffie Hellman (DH) oraz Elliptic-Curve Diffie Hellman (ECDH)</li> <li>f. wsparcie dla Elliptic Curve Digital Signature Algorithm (ECDSA) (256-bit i 384-bit) dla podpisu certyfikatów X.509</li> <li>g. wsparcie dla walidacji certyfikatów X.509 z użyciem ECDSA</li> <li>h. wsparcie dla Message Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 i 2 (SHA-1 i SHA-2) i AES-GMAC (128-, 192-, 256- bitów)</li> </ul>
UB D 14	Urządzenie musi zapewniać możliwość konfiguracji tuneli IPv4 IPsec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2) dla rozwiązań typu DMVPN (lub równoważnych)
UB D 15	Urządzenie musi zapewniać możliwość szyfrowanie ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem protokołu Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547
UB D 16	<p>Urządzenie musi umożliwiać akcelerację ruchu sieciowego TCP w kierunku od klienta do serwera oraz od serwera do klienta wykorzystując co najmniej następujące mechanizmy:</p> <ul style="list-style-type: none"> <li>a. Bezstratną kompresję danych</li> <li>b. Cache'owanie danych w warstwie transportowej (niezależne od typu aplikacji)</li> <li>c. Manipulację parametrami protokołu TCP</li> </ul>
UB D 17	Urządzenie musi umożliwiać optymalizację co najmniej następujących protokołów aplikacyjnych, przy czym przez optymalizację rozumie się ingerowanie w warstwę

	<p>aplikacyjną protokołu w celu poprawy jego działania:</p> <p>a. CIFS/SMBv1</p> <p>b. HTTP</p>
UB D 18	Urządzenie musi umożliwiać rozszyfrowywanie i akcelerację ruchu sieciowego zaszyfrowanego przy pomocy protokołu SSL/TLS z zachowaniem natywnych mechanizmów szyfrowania
UB D 19	Urządzenie musi wykonywać akcelerację i optymalizację w sposób transparentny z zachowaniem oryginalnego płaczenia TCP
UB D 20	Możliwość równoczesnej akceleracji minimum 400 połączeń
UB D 21	Router musi mieć możliwość zarządzania poprzez CLI (konsola szeregową, SSHv2) i SNMPv3
UB D 22	Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika
UB D 23	Plik konfiguracyjny urządzenia musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych (do wielkości pamięci flash). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian
UB D 24	Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora
UB D 25	Urządzenie musi oferować dla pakietów o długości 64 bajtów wydajność co najmniej 950 kpps
UB D 26	Router z uruchomionymi usługami powinien zapewniać wydajność co najmniej 150Mb/s (zgodnie z danymi i zaleceniami producenta)
UB D 27	Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i Dense) oraz routing statyczny
UB D 28	Protokół BGP musi posiadać obsługę 4 bajtowych ASN
UB D 29	Musi posiadać wsparcie dla funkcjonalności Policy Based Routing
UB D 30	Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2



UB D 31	Musi posiadać wsparcie dla protokołu DVMRP
UB D 32	Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
UB D 33	Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q
UB D 34	Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
UB D 35	Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router)
UB D 36	Musi posiadać obsługę NAT i PAT. Mechanizm NAT musi zapewniać wsparcie dla H.224/H.245
UB D 37	Musi posiadać wsparcie dla protokołów WCCP i WCCPv2 (lub równoważnych)
UB D 38	Musi posiadać obsługę wirtualnych instancji routingu (VRF)
UB D 39	Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu
UB D 40	Musi zapewniać obsługę mechanizmów kolejkowania ruchu: <ul style="list-style-type: none"> <li>a. z obsługą kolejki absolutnego priorytetu</li> <li>b. ze statyczną alokacją pasma dla typu ruchu</li> <li>c. WFQ</li> </ul>
UB D 41	Musi obsługiwać mechanizm WRED
UB D 42	Musi obsługiwać protokół RSVP
UB D 43	Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
UB D 44	Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precedence dla ruchu tunelowanego
UB D 45	Musi obsługiwać protokół NTP
UB D 46	Musi obsługiwać DHCP w zakresie Client, Server
UB D 47	Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika)
UB D 48	Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+

UB D 49	Musi posiadać funkcjonalność stateful firewall (w trybie routed oraz transparent)
UB D 50	<p>Urządzenie musi posiadać możliwość rozbudowy (poprzez zakup odpowiedniej licencji lub wymianę oprogramowanie bez konieczności zmian sprzętowych) o wsparcie dla:</p> <ul style="list-style-type: none"> <li>a. MPLS (funkcje LER i LSR), MPLS Traceroute, Traffic Engineering (w tym Fast Reroute, Link i Node Protection), Multicast dla MPLS VPN</li> <li>b. systemu IPS</li> <li>c. możliwość procesowania połączeń telefonii IP (funkcja serwera zestawiającego połączenia) dla co najmniej 350 abonentów</li> <li>d. możliwość współpracy z centralnym systemem procesowania połączeń telefonii IP w celu przejęcia podstawowych funkcji telefonii do połączeń wewnętrznych oraz wyjścia na linie miejskie na czas awarii połączenia do systemu centralnego. Funkcja ta musi być w stanie obsłużyć co najmniej 350 abonentów</li> <li>e. możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów PRI/BRI lub analogowych – po doposażeniu w odpowiednie interfejsy i moduły DSP (ich dostarczenie nie jest częścią tego postępowania)</li> <li>f. możliwość pracy jako mostek do połączeń VoIP wielopunktowych</li> <li>g. funkcjonalność Gatekeeper'a H.323</li> <li>h. możliwość działania jako brama IP-do-IP dla połączeń głosowych i wideo realizowanych w sieci IP</li> <li>i. funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia „tam i z powrotem” (roundtrip), jitter i utraty pakietów)</li> </ul>

Urządzenia kontroli treści typu D	
Wymaganie	Minimalne wymagania dotyczące Urządzeń kontroli treści (UTM) typu D
UTM D	<b>Dla lokalizacji posiadających powyżej 300 użytkowników, Wykonawca zapewni sprzęt posiadający wszystkie poniższe właściwości:</b>
UTM D 1	Rozwiązanie powinno dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
UTM D 2	System realizujący funkcję Firewall powinien dysponować minimum 20 interfejsami miedzianymi Ethernet 10/100/1000 pracującymi niezależnie.
UTM D 3	Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy

	w oparciu o standard 802.1Q.
UTM D 4	W zakresie Firewall'a obsługa nie mniej niż 2,5 milion jednoczesnych połączeń oraz 22 tys. nowych połączeń na sekundę.
UTM D 5	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> <li>A) Kontrola dostępu – zaporą ogniową klasy Stateful Inspection.</li> <li>B) Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.</li> <li>C) Poufność danych - IPSec VPN oraz SSL VPN.</li> <li>D) Ochrona przed atakami - Intrusion Prevention System [IPS/IDS].</li> <li>E) Kontrola stron Internetowych – Web Filter [WF].</li> <li>F) Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP).</li> <li>G) Kontrola pasma oraz ruchu [QoS i Traffic shaping].</li> <li>H) Kontrola aplikacji oraz rozpoznawanie ruchu P2P.</li> <li>I) Możliwość analizy ruchu szyfrowanego SSL'em.</li> <li>J) Ochrona przed wyciekiem poufnej informacji (DLP).</li> <li>K) Wydajność systemu Firewall min 200Mbps dla pakietów 64 bajtowych.</li> </ul>
UTM D 6	Aktualizacja baza sygnatur wirusów musi być zapewniona na okres min 5 lat od dnia dokonania odbioru końcowego.
UTM D 7	Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 700 Mbps
UTM D 8	Wydajność ochrony przed atakami (IPS) min 950 Mbps.
UTM D 9	Wydajność szyfrowania IPSec, nie mniej niż 450 Mbps
UTM D 10	<p>W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:</p> <ul style="list-style-type: none"> <li>A) Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.</li> <li>B) Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem.</li> <li>C) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>D) Praca w topologii Hub and Spoke oraz Mesh.</li> </ul>

	<p>E) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF.</p> <p>F) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.</p>
UTM D 11	Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
UTM D 12	Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
UTM D 13	Możliwość budowy min 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
UTM D 14	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
UTM D 15	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
UTM D 16	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
UTM D 17	Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
UTM D 18	Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
UTM D 19	Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 55 kategorii (np. IT, Zakupy). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
UTM D 20	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
UTM D 21	Wymaga się aby dostarczony system oferował możliwość uruchomienia funkcjonalności optymalizacji ruchu WAN, korzystającą minimum z techniki byte-

	caching, w celu jak najlepszego wykorzystania dostępnych łącz internetowych.
UTM D 22	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: <ul style="list-style-type: none"> <li>A) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>B) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>C) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> <li>D) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory.</li> </ul>
UTM D 23	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: <ul style="list-style-type: none"> <li>A) ICSA lub EAL4 – dla funkcjonalności Firewall.</li> </ul>
UTM D 24	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
UTM D 25	Wymaga się, aby system był wyposażony w przestrzeń dla lokalnego logowania zdarzeń o pojemności min 8 GB.

### 12.1.7 Funkcjonalność oprogramowania w urządzeniach bezpieczeństwa typu A,B,C,D

Funkcjonalność oprogramowania w urządzeniach bezpieczeństwa urządzeniach typu A,B,C,D	
Wymaganie	Minimalne wymagania dotyczące Funkcjonalności oprogramowania firewalli w urządzeniach typu A,B,C,D
FOF 1	Rozwiązanie musi być oparte o dedykowany system operacyjny – 64 bitowy. Nie dopuszcza się rozwiązań gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim posadowione oprogramowanie firewall (jako aplikacja).
FOF 2	Rozwiązanie musi posiadać funkcjonalność ściany ogniowej śledzącej stan połączeń (w warstwach 3 i 4 modelu OSI) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.

FOF 3	Rozwiązanie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
FOF 4	Rozwiązanie musi pozwalać na definiowanie firewalli w trybie warstwy 3 (routed) i warstwy 2 transparentnym (w warstwie L2 OSI).
FOF 5	Rozwiązanie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory lub równoważny.
FOF 6	Rozwiązanie musi pozwalać na wirtualizację konfiguracji poprzez wirtualne firewalle/konteksty/domeny. Wymagana jest obsługa co najmniej 2 wirtualnych kontekstów Firewall oraz możliwość rozszerzenia ilości obsługiwanych wirtualnych kontekstów Firewall do co najmniej 10.
FOF 7	Rozwiązanie musi zapewnić mechanizmy inspekcji aplikacyjnej i kontroli następujących usług: <ul style="list-style-type: none"> <li>A) Hypertext Transfer Protocol (HTTP),</li> <li>B) File Transfer Protocol (FTP),</li> <li>C) Simple Mail Transfer Protocol (SMTP),</li> <li>D) Domain Name System (DNS),</li> <li>E) H.323,</li> <li>F) Session Initiation Protocol (SIP),</li> <li>G) Lightweight Directory Access Protocol(LDAP),</li> <li>H) Internet Control Message Protocol (ICMP),</li> <li>I) Network File System (NFS).</li> </ul>
FOF 8	Rozwiązanie musi zapewniać mechanizmy pozwalające na blokowanie aplikacji tunelowanych z użyciem wybranego portu (np. 80)w tym: <ul style="list-style-type: none"> <li>A) blokowanie komunikatorów internetowych,</li> <li>B) blokowanie aplikacji typu peer-to-peer .</li> </ul>
FOF 9	Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego OSPF oraz RIPv2.
FOF 10	Rozwiązanie musi zapewniać obsługę ruchu multicast w tym <ul style="list-style-type: none"> <li>A) Protokoły routingu multicast (PIM),</li> <li>B) IGMP,</li> <li>C) definiowanie list kontroli dostępu dla ruchu multicast.</li> </ul>
FOF 11	Rozwiązanie musi zapewniać obsługę ruchu z adresacją IPv6

	<p>A) pracę w sieci z adresacją IPv6,</p> <p>B) definiowanie list kontroli dostępu dla ruchu IPv6,</p> <p>C) inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń,</p> <p>D) Hop-by-Hop Options,</p> <p>E) Routing (Type 0),</p> <p>F) Fragment,</p> <p>G) Destination Options,</p> <p>H) Authentication,</p> <p>I) Encapsulating Security Payload,</p> <p>J) zarządzanie urządzeniem poprzez SSHv2, HTTPS w sieci IPv6.</p>
FOF 12	Rozwiązanie musi umożliwiać zestawienie sesji IPsec VPN i WebVPN.
FOF 13	Rozwiązanie musi obsługiwać IKE i IKEv2.
FOF 14	Rozwiązanie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPsec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat).
FOF 15	Rozwiązanie musi obsługiwać współpracę z serwerami certyfikatów (CA).
FOF 16	Rozwiązanie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS.
FOF 17	Rozwiązanie musi posiadać możliwość wyeksportowania konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.
FOF 18	Rozwiązanie powinno być zarządzane przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.

## 12.2 Wymagania ogólne dla dostarczanych rozwiązań

Wymagania ogólne dla dostarczanych rozwiązań	
Wymaganie	Minimalne wymagania
	<b>Zamawiający wymaga by:</b>
WO 1	Całość dostarczanego sprzętu i oprogramowania pochodziła z autoryzowanego kanału sprzedaży producentów – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy.
WO 2	Dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na

	6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu realizacji procedur opisanych w zakresie Zamówienia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).
WO 3	<p>Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne Wykonawcy w okresie wymaganym w SIWZ. Jeżeli zgodnie z licencją producenta aktualizacja oprogramowania wymaga wykupienia odpowiedniego wsparcia u producenta to Wykonawca powinien takie wsparcie wykupić.</p> <p>Jeżeli do poprawnego działania wymaganych funkcjonalności konieczne jest wykupienie subskrypcji to Wykonawca powinien ją zapewnić na cały okres świadczenia usług gwarancyjnych..</p>
WO 4	Ze względu na pożądaną pełną kompatybilność oraz zabezpieczenie uprawnień gwarancyjnych Zamawiającego, dostarczane w ramach Zamówienia rozwiązania (urządzenia oraz karty i moduły do nich) powinny pochodzić od jednego producenta, chyba że wymagania szczegółowe stanowią inaczej.
WO 5	<p>W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:</p> <ul style="list-style-type: none"> <li>A) zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację),</li> <li>B) zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych.</li> <li>C) Jeżeli inspekcja, o której mowa powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 20% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Stronę w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych.</li> </ul>



WO 6	Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert.
WO 7	Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.

## 13 Wyposażenie urzędów JST w sprzęt i urządzenia

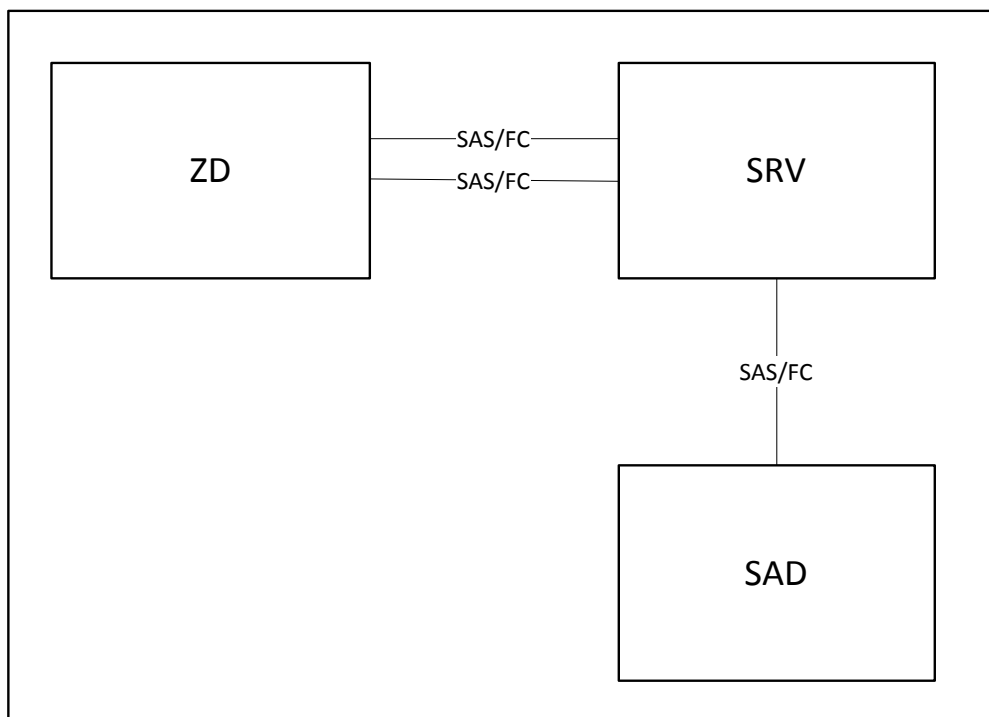
### 13.1 Dostawa i uruchomienie serwerów

Celem realizacji projektu w zakresie dostawy i uruchomienia serwerów jest wyposażenie JST biorących udział w projekcie PSeAP w nowoczesne zestawy serwerowe zapewniające funkcjonowanie SEOD. W zależności od liczby użytkowników SEOD w danej JST planuje się dostawę zestawu serwerowego w następujących wariantach:

- Typ A: od 0 do 50 użytkowników,
- Typ B: od 51 do 150 użytkowników,
- Typ C: powyżej 150 użytkowników.

### 13.2 Oznaczenia i definicje

Schemat blokowy, oznaczenia i skróty literowe



Rysunek 7 Poglądowy schemat połączeń architektury ZESTAWÓW SERWEROWYCH JST. Identyfikacyjny dla zestawów TYP A, B i C

Oznaczenia:

ZD – ZASÓB DYSKOWY

SRV – SERWER

SAD – SYSTEM ARCHIWIZACJI DANYCH

SAS/FC – Połączenie realizowane w technologii SAS lub FC o przepustowości co najmniej 6Gb/s

### **Standaryzacja PRZEPUSTOWOŚCI**

W celu uniknięcia nieporozumień związanych z pojęciem przepustowości, które użyte jest w późniejszym tekście wymagań Zamawiający podajewartości, które należy przyjąć przy obliczaniu przepustowości na potrzeby niniejszej specyfikacji.

**Tabela 2 Zestawienie Przepustowości**

standard	Przepustowość [Gb/s]
DDR3-1066 ; -1333 ; -1600	8,5 ; 10,6 ; 12,8 [GB/s]
10 Gb Ethernet ; 1 Gb Ethernet	10 ; 1
8 Gb ; 4 Gb FC	8 ; 4
QDR ;DDR ; SDR InfiniBand	10 ; 5 ; 2,5
EDR ; FDR Infiniband	26 ; 14
6G ; 3G SAS	6 ; 3
6G ; 3G ; 1,5 SATA	6 ; 3 ; 1,5

Jeśli port używa zwielokrotnionych linii jego przepustowość na potrzeby niniejszej specyfikacji należy przyjąć jako iloczyn liczby linii i wyżej podanej przepustowości (przykład: przepustowość 4X QDR INFINIBAND na potrzeby niniejszej specyfikacji wynosi 40 Gb/s).

Jeśli transmisja na linii zachodzi równocześnie w dwu kierunkach to dla potrzeb niniejszej specyfikacji należy przyjąć nie wartość dwukrotnie wyższą, ale dokładnie taką jaką znajduje się podanej tabeli.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego przepustowość jest oznaczana dużą literą (PRZEPUSTOWOŚĆ) w odróżnieniu od innych przepustowości.

### **Równoważność kanałów komunikacyjnych**

W miejscach gdzie Zamawiający wyspecyfikował rodzaj kanału komunikacyjnego jako równoważny kanał komunikacyjny Zamawiający dopuszcza kanał komunikacyjny o IDENTYCZNYM protokole, ale o większej prędkości. Zamawiający nie dopuszcza innego niż wyspecyfikowany protokołu pomimo, że zamienny protokół będzie posiadał większą PRZEPUSTOWOŚĆ.

Przykład:

- Dla wymagania ETHERNET 10Gb jako równoważne NIE JEST akceptowane połączenie o większej PRZEPUSTOWOŚCI, ale jedynie o większej prędkości. W tym wypadku ETHERNET 40 Gb lub 100 Gb.
- Analogicznie dla wymagania FC 8Gb jako równoważne AKCEPTOWANE jest jedynie połączenie FC, ale o większej prędkości. W tym wypadku FC 16Gb lub więcej.

### **Definicja pojęcia MOC OBLICZENIOWA**

Wzór 1. Maksymalna (szczytowa) teoretyczna moc obliczeniowa procesora

$$R_{proc} = C * I * F,$$

gdzie:

R<sub>proc</sub> - moc obliczeniowa w GFlops

C- liczba dzeni procesora

I- liczba instrukcji zmiennoprzecinkowych typu dodawanie i mnożenie w podwójnej precyzji wykonywanych przez pojedynczy dzień procesora w czasie jednego cyklu zegarowego (np. dla procesora Intel Xeon (seria 5600) I wynosi 4, dla procesorów AMD Opteron I wynosi 4),

F- częstotliwość zegara procesora w GHz.

Dla potrzeb niniejszej specyfikacji Zamawiający jako częstotliwość zegara przyjmuje nominalną częstotliwość zegara procesora podawaną przez producenta procesora przy handlowym opisie procesora. Pomimo, że procesor może pracować z częstotliwością niższą lub wyższą niż wyżej wspomniana częstotliwość jako częstotliwość do obliczenia mocy obliczeniowej procesora w niniejszej specyfikacji należy przyjąć właśnie częstotliwość podawaną przy opisach handlowych przez producentów procesorów.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego moc obliczeniowa zdefiniowana we wzorze 1 i opisana w niniejszym akapicie jest oznaczana dużą literą (MOC OBLICZENIOWA) w odróżnieniu od innych mocy obliczeniowych.

### **Konwencja zapisów**

- I) Zapis „SAS / FC” lub „USB / SD” użyty w dalszej części specyfikacji oznacza jedną z dwóch technologii: albo SAS albo FC, albo USB albo SD.
- II) Nazwy pisane z dużej litery są stosowanymi na potrzeby niniejszej specyfikacji nazwami własnymi np. Serwer BLADE, Lokalne Dyski.
- III) Słowa „LUB” lub „ALBO” napisane z dużej litery oznaczają kwalifikator logiczny i nie są używane w potocznym znaczeniu.

Przykład:

- a) Jeśli Zamawiający wymaga odporności Systemu na awarię elementu A ALBO elementu B oznacza to, że System nie musi być odporny na RÓWNOCZESNĄ awarię elementu A i elementu B.
- b) Jeśli Zamawiający wymaga odporności systemu na awarię elementu A LUB elementu B oznacza to, że system nie tylko ma być odporny na awarię jednego z dwu elementów A albo B, ale też musi być odporny na równoczesną awarię obu elementów i A i B.

## **Wymagania ogólne**

### **Jakość sprzętu**

- a) Cały dostarczony sprzęt musi być fabrycznie nowy, tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów jego poprawnej pracy.
- b) Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.

## **13.3 Opis wymagań sprzętowych**

### **13.3.1 Zestaw serwerowy – wariant A**

Przez zestaw serwerowy wariant A Zamawiający rozumie zestaw składający się z co najmniej:

- serwera obliczeniowego spełniającego wymagania opisane w punkcie 13.3.1.1 niniejszej specyfikacji,
- zasobu dyskowego spełniającego wymagania opisane w punkcie 13.3.1.2 niniejszej specyfikacji,
- systemu archiwizacji danych składającego się z urządzenia do archiwizacji danych opisanego w punkcie 13.2.1.3 niniejszego OPZ.

Zamawiający wymaga aby suma mocy obliczeniowej serwerów w tej kategorii wynosiła dla każdej lokalizacji 332,8 Gflops lub więcej.

#### **13.3.1.1 Serwer OBLICZENIOWY wariant A**

<b>Serwer OBLICZENIOWY wariant A</b>	
<b>Parametr</b>	<b>Charakterystyka (wymagania minimalne)</b>
SO A 1	Serwer OBLICZENIOWY wariant A musi spełniać niżej wymienione wymagania:
SO A 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 2U.
SO A 2	A) Wszystkie procesory Serwerów OBLICZENIOWYCH muszą być identyczne. B) Procesory muszą być typu x86, wykonywać instrukcje 64 bitowe oraz zawierać na sobie kontroler pamięci RAM.



	<p>C) Zainstalowane co najmniej 2 procesory</p> <p>D) Suma wydajności procesorów musi wynosić:</p> <ul style="list-style-type: none"><li>i SPECint_base2006 <math>\geq</math> 49.8</li><li>ii SPECfp_base2006 <math>\geq</math> 79.7</li></ul> <p>Zamawiający wymaga, by dla zaoferowanego zestawu serwerów na stronie <a href="http://www.spec.org">www.spec.org</a> opublikowane były wyniki testów wydajności, potwierdzające spełnienie obu powyższych warunków dotyczących wydajności. Zamawiający dopuszcza, by wyniki te dotyczyły serwera innego producenta, serwera o innej konfiguracji lub innego modelu serwera niż oferowany serwer, pod warunkiem jednak, że serwer ten posiada taki sam zestaw procesorów co oferowany serwer.</p>
SO A 3	<p>A) musi posiadać 24 GB lub więcej pamięci RAM.</p> <p>B) Wszystkie moduły pamięci RAM wszystkich SERWERÓW muszą być identycznie między sobą.</p> <p>C) Musi istnieć możliwość rozbudowy do co najmniej 384GB pamięci RAM dla każdego zainstalowanego procesora.</p> <p>D) Pamięć z technologią ECC.</p>
SO A 4	<p>Nadmiarowy, odporny na awarię 1 szt. zasilacza system, który spełnia następujące wymagania:</p> <ul style="list-style-type: none"><li>A) Wymienny z zewnątrz, podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</li><li>B) W ilości maksymalnej dla obudowy przewidzianej przez producenta obudowy.</li></ul>
SO A 5	<p>Nadmiarowy, odporny na awarię 1 szt. wiatraka system, który spełnia następujące wymagania:</p> <ul style="list-style-type: none"><li>A) Wymienny podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</li><li>B) W ilości maksymalnej dla obudowy przewidzianej przez producenta obudowy.</li></ul>
SO A 6	<p>Musi posiadać co najmniej jeden napęd DVD-ROM</p>
SO A 7	<p>Zamawiający wymaga by każdy SERWER posiadał niżej wyspecyfikowane porty. Zamawiający nie dopuszcza by jakiegokolwiek typ portu był przeznaczony do użycia w dwu lub więcej wymaganych standardach.</p> <p><u>Standard SAS 6G:</u></p> <ul style="list-style-type: none"><li>A) 1 para (2szt.) portów lub więcej par portów dokładnie SAS 6G.</li><li>B) standard portów umożliwiający połączenie z SYSTEMEM ARCHIWIZACJI DANYCH Wariant A opisanym poniżej.</li></ul> <p><u>Standard ETHERNET 1Gb</u></p>

	<p>A) 2 pary (4szt.) portów lub więcej par portów o przepustowości co najmniej 1Gb ETHERNET każdy.</p> <p>B) Wszystkie wymagane porty muszą być aktywne i umożliwiać połączenie do infrastruktury Zamawiającego.</p> <p>C) Każdy z portów musi posiadać wsparcie dla standardów: PXE oraz mechanizmów odciążenia procesora LargeSendOffload (LSO),SegmentationOffload (TSO) oraz CheksumOffload (CSO).</p> <p><u>Standard USB/SD:</u></p> <p>A) 4 szt. portu lub więcej pracującego w standardzie USB lub SD.</p> <p>B) Co najmniej jeden z portów dostępny wewnątrz obudowy serwera.</p>
SO A 8	<p>Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na:</p> <p>A) włączenie, wyłączenie i restart serwera,</p> <p>B) podgląd logów sprzętowych serwera i karty,</p> <p>C) przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu i restartu OS),</p> <p>D) możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów.</p> <p>Rozwiązanie musi być niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.</p>

### 13.3.1.2 Zasób Dyskowy wariant A

Zamawiający wymaga dostarczenia co najmniej jednej sztuki (1 szt.) Zasobu Dyskowego Wariant A dla każdego z oferowanych serwerów obliczeniowych Wariant A

Zasób Dyskowy wariant A	
Parametr	Charakterystyka (wymagania minimalne)
ZD A 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 2U.
ZD A 2	<p>Każdy oferowany zasób dyskowy musi udostępniać co najmniej 2,4 TB przestrzeni dyskowej w postaci co najmniej 8 szt. identycznych dysków twardych o parametrach:</p> <p>A) Prędkość obrotowa 15.000 [RPM] o przepustowości minimum 6Gbit/s lub więcej z minimalnymi transferami 100 MB/s dla sekwencyjnego odczytu oraz 80 MB/s zapisu sekwencyjnego ALBO w technologii SSD z minimalnymi transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</p> <p>B) Wyposażony w 1 parę (2 szt.) portów SAS 6G / FC 8G. Awaria jednego portu</p>

	<p>z pary nie przerywa dostępu do danych znajdujących się na dysku.</p> <p>Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują.</p>
ZD A 3	<p>Udostępnianie przestrzeni dyskowej musi odbywać się przy wykorzystaniu:</p> <ul style="list-style-type: none"> <li>A) Co najmniej 1 sztuki kontrolera wyposażonego w co najmniej 1 parę (2szt.) portów SAS 6G / FC 8G.</li> <li>B) Każdy z kontrolerów wyposażony w co najmniej 2 GB pamięci podręcznej, buforującej zapisy i odczyty. Pamięć nieulotna dostępna jednocześnie dla wszystkich zainstalowanych dysków twardych.</li> </ul>
ZD A 4	<p>Oferowany zasób dyskowy musi posiadać funkcjonalność:</p> <ul style="list-style-type: none"> <li>A) Tworzenia jednego z wybranych poziomów sprzętowych RAID 0,1,1+0,5,5+0 na wszystkich dostępnych dyskach twardych jednocześnie, bez wykorzystania systemu operacyjnego.</li> <li>B) Startu systemu operacyjnego rodziny Windows lub Linux.</li> <li>C) Tworzenie Globalnego dysku spare.</li> <li>D) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</li> </ul>
ZD A 5	<p>Zarządzania za pomocą GUI oraz CLI o funkcjonalności co najmniej:</p> <ul style="list-style-type: none"> <li>A) Panel GUI dostępny z poziomu systemu Linux oraz Windows.</li> <li>B) Tworzenia sprzętowych poziomów RAID 0,1,1+0,5,5+0.</li> <li>C) Tworzenia/usuwanie Globalnego dysku spare.</li> <li>D) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</li> <li>E) Dynamiczną zmianę wielkości wolumenów logicznych LUN, bez przerywania dostępu do danych znajdujących się na dyskach.</li> </ul>

### 13.3.1.3 System Archiwizacji DANYCH Wariant A

Zamawiający wymaga dostarczenia co najmniej jednej sztuki (1 szt.) Systemu Archiwizacji DANYCH dla każdego oferowanego serwera obliczeniowego wariant A składającego się na autoloader oraz oprogramowanie zarządzające tworzeniem kopii zapasowych.

Ponadto każdy z oferowanych Systemów Archiwizacji DANYCH wariant A musi spełniać poniższe warunki:

System Archiwizacji Danych Wariant A	
Parametr	Charakterystyka (wymagania minimalne)
SAD A 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 1U.

SAD A 2	System musi posiadać co najmniej 8 slotów przeznaczonych na zestaw taśm składających się z: A) 8 sztuk taśm w standardzie LTO5 lub lepszym o pojemności co najmniej 3 TB każda, B) 1 szt. taśmy czyszczącej, C) zestawu kodów kreskowych w celu identyfikacji każdej z dostarczonych taśm.
SAD A 3	System musi posiadać co najmniej 1 port SAS 6G w standardzie umożliwiającym podłączenie do portu Serwera OBLICZENIOWEGO Wariant A opisanego w punkcie 13.3.1.1 niniejszej specyfikacji.
SAD A 4	System musi posiadać w co najmniej 1 napęd o parametrach: A) standard LTO5 lub lepszy, B) przepustowość co najmniej 980 GB/hr.

### 13.3.2 Zestaw serwerowy – wariant B

Przez Zestaw serwerowy wariant B Zamawiający rozumie zestaw składający się z co najmniej:

- serwera obliczeniowego spełniającego wymagania opisane w punkcie 13.3.2.1 niniejszej specyfikacji,
- zasobu dyskowego spełniającego wymagania opisane w punkcie 13.3.2.2 niniejszego OPZ
- systemu archiwizacji danych składającego się z urządzenia do archiwizacji danych opisanego w punkcie 13.3.2.3 niniejszego OPZ

Zamawiający wymaga aby suma mocy obliczeniowej serwerów w tej kategorii wynosiła dla każdej lokalizacji 332,8Gflops lub więcej.

- Zamawiający wymaga aby każdy z dostarczonych Zestawów Serwerowych Wariant B posiadał identyczną konfigurację i spełniał wymagania opisane w punkcie 13.3.2.1. niniejszego OPZ.

#### 13.3.2.1 Serwer OBLICZENIOWY wariant B

Serwer OBLICZENIOWY wariant B	
Parametr	Charakterystyka (wymagania minimalne)
SO B 1	Serwer OBLICZENIOWY wariant B musi posiadać obudowę dedykowaną do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych o wielkości nie większej niż 2U.
SO B 2	A) Wszystkie procesory Serwerów OBLICZENIOWYCH muszą być identyczne. B) Procesory muszą być typu x86, wykonywać instrukcje 64 bitowe oraz zawierać na sobie kontroler pamięci RAM. C) Zainstalowane co najmniej 2 procesory.





	<p>D) Suma wydajności procesorów musi wynosić:</p> <ul style="list-style-type: none"><li>i SPECint_base2006 <math>\geq</math> 49.8,</li><li>ii SPECfp_base2006 <math>\geq</math> 79.7.</li></ul> <p>Zamawiający wymaga, by dla zaoferowanego zestawu serwerów na stronie <a href="http://www.spec.org">www.spec.org</a> opublikowane były wyniki testów wydajności, potwierdzające spełnienie obu powyższych warunków dotyczących wydajności. Zamawiający dopuszcza, by wyniki te dotyczyły serwera innego producenta, serwera o innej konfiguracji lub innego modelu serwera niż oferowany serwer, pod warunkiem jednak, że serwer ten posiada taki sam zestaw procesorów co oferowany serwer.</p>
SO B 3	<p>A) Serwer OBLICZENIOWY wariant B musi posiadać 48 GB lub więcej pamięci RAM.</p> <p>B) Wszystkie moduły pamięci RAM wszystkich SERWERÓW muszą być identycznie między sobą.</p> <p>C) Możliwość rozbudowy do co najmniej 384GB pamięci RAM dla każdego zainstalowanego procesora.</p> <p>D) Pamięć z technologią ECC.</p>
SO B 4	<p>Nadmiarowy, odporny na awarię 1 szt. zasilacza system, który spełnia następujące wymagania:</p> <p>A) Wymienny z zewnątrz, podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</p> <p>B) W ilości maksymalnej dla obudowy przewidzianej przez producenta obudowy.</p>
SO B 5	<p>Nadmiarowy, odporny na awarię 1 szt. wiatraka system, który spełnia następujące wymagania:</p> <p>A) Wymienny podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</p> <p>B) W ilości maksymalnej dla obudowy przewidzianej przez producenta obudowy.</p>
SO B 6	<p>Serwer OBLICZENIOWY wariant B musi posiadać co najmniej jeden napęd DVD-ROM.</p>
SO B 7	<p>Zamawiający wymaga by każdy Serwer OBLICZENIOWY wariant B posiadał niżej wyspecyfikowane porty. Zamawiający nie dopuszcza by jakiegokolwiek typ portu był przeznaczony do użycia w dwu lub więcej wymaganych standardach.</p> <p><u>standard SAS 6G:</u></p> <p>A) 1 para (2szt.) portów lub więcej par portów dokładnie SAS 6G.</p> <p>B) standard portów umożliwiający połączenie z SYSTEMEM ARCHIWIZACJI DANYCH Wariant B opisanym poniżej.</p>

	<p><u>standard ETHERNET 1Gb</u></p> <p>A) 2 pary (4szt.) portów lub więcej par portów o przepustowości co najmniej 1Gb ETHERNET każdy.</p> <p>B) Wszystkie wymagane porty muszą być aktywne i umożliwiać połączenie do infrastruktury Zamawiającego.</p> <p>C) Każdy z portów musi posiadać wsparcie dla standardów: PXE oraz mechanizmów odciążenia procesora LargeSendOffload (LSO),SegmentationOffload (TSO) oraz CheksumOffload (CSO).</p> <p><u>standard USB/SD:</u></p> <p>A) 4 szt. portu lub więcej pracującego w standardzie USB lub SD.</p> <p>B) Co najmniej jeden z portów dostępny wewnątrz obudowy serwera.</p>
SO B 8	<p>Serwer OBLICZENIOWY wariant B musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na:</p> <p>A) włączenie, wyłączenie i restart serwera,</p> <p>B) podgląd logów sprzętowych serwera i karty,</p> <p>C) przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu i restartu OS),</p> <p>D) możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów.</p> <p>Rozwiązanie musi być niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.</p>

### 13.3.2.2 Zasób Dyskowy wariant B

Zamawiający wymaga dostarczenia co najmniej jednej sztuki (1sz) Zasobu Dyskowego Wariant B do każdego z oferowanych serwerów Wariant B. Ponadto każdy z oferowanych Zasobów Dyskowych Wariant B musi spełniać poniższe warunki:

Zasób Dyskowy wariant B	
Parametr	Charakterystyka (wymagania minimalne)
ZD B 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 2U.
ZD B 2	<p>Każdy oferowany ZASÓB DYSKOWY musi udostępniać co najmniej 4,8 TB przestrzeni dyskowej w postaci co najmniej 8 szt. identycznych dysków twardych o parametrach:</p> <p>A) Prędkość obrotowa 10.000 [RPM] o przepustowości minimum 6Gbit/s lub więcej z minimalnymi transferami 100 MB/s dla sekwencyjnego odczytu oraz 80 MB/s zapisu sekwencyjnego ALBO w technologii SSD z minimalnymi</p>

	<p>transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</p> <p>B) Wyposażony w 1 parę (2 szt.) portów SAS 6G / FC 8G. Awaria jednego portu z pary nie przerywa dostępu do danych znajdujących się na dysku.</p> <p>Zasób Dyskowy wariant B musi umożliwiać rozbudowę do co najmniej 16 sztuk dysków twardych. Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują.</p>
ZD B 3	<p>Udostępnianie przestrzeni dyskowej musi odbywać się przy wykorzystaniu:</p> <p>A) Co najmniej 1 sztuki kontrolera wyposażonego w co najmniej 1 parę (2szt.) portów SAS 6G / FC 8G.</p> <p>B) Każdy z kontrolerów wyposażony w co najmniej 2 GB pamięci podręcznej, buforującej zapisy i odczyty. Pamięć nieulotna dostępna jednocześnie dla wszystkich zainstalowanych dysków twardych.</p>
ZD B 4	<p>Oferowany zasób dyskowy musi posiadać funkcjonalność:</p> <p>A) Tworzenia jednego z wybranych poziomów RAID 0,1,1+0,5,5+0 na wszystkich dostępnych dyskach twardych jednocześnie.</p> <p>B) Tworzenie Globalnego dysku spare.</p> <p>C) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</p>
ZD B 5	<p>Zarządzania za pomocą GUI oraz CLI o funkcjonalności co najmniej:</p> <p>A) Tworzenia poziomów RAID 0,1,1+0,5,5+0.</p> <p>B) Tworzenia/usuwanie Globalnego dysku spare.</p> <p>C) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</p> <p>D) Dynamiczną zmianę wielkości wolumenów logicznych LUN, bez przerywania dostępu do danych znajdujących się na dyskach.</p>

### 13.3.2.3 System Archiwizacji DANYCH Wariant B

Zamawiający wymaga dostarczenia co najmniej jednej sztuki (1 szt.) Systemu Archiwizacji DANYCH dla każdego oferowanego serwera OBLICZENIOWEGO wariant B składającego się na autoloader oraz oprogramowanie zarządzające tworzeniem kopii zapasowych.

Ponadto każdy z oferowanych Systemów Archiwizacji DANYCH wariant B musi spełniać poniższe warunki:

System Archiwizacji DANYCH Wariant B	
Parametr	Charakterystyka (wymagania minimalne)
SAD B 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do

	mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 1U.
SAD B 2	System musi posiadać co najmniej 8 slotów przeznaczonych na zestaw taśm składających się z: <ul style="list-style-type: none"> <li>A) 8 sztuk taśm w standardzie LTO5 lub lepszym o pojemności co najmniej 3 TB każda,</li> <li>B) 1 szt. taśmy czyszczącej,</li> <li>C) zestawu kodów kreskowych w celu identyfikacji każdej z dostarczonych taśm.</li> </ul>
SAD B 3	System musi posiadać co najmniej 1 port SAS 6G w standardzie umożliwiającym podłączenie do portu Serwera obliczeniowego wariant B opisanego w punkcie 13.3.2.1 niniejszej specyfikacji.
SAD B 4	System musi być wyposażony w co najmniej 1 napęd o parametrach: <ul style="list-style-type: none"> <li>A) standard LTO5 lub lepszy,</li> <li>B) przepustowość co najmniej 980 GB/hr.</li> </ul>

### 13.3.3 Zestaw serwerowy – wariant C

Przez Zestaw serwerowy wariant C Zamawiający rozumie zestaw składający się z co najmniej:

- serwera obliczeniowego spełniającego wymagania opisane w punkcie 13.3.3.1 niniejszego OPZ
- zasobu dyskowego spełniającego wymagania opisane w punkcie 13.3.3.2 niniejszego OPZ
- systemu archiwizacji danych składającego się z urządzenia do archiwizacji danych opisanego w punkcie 13.3.3.3 niniejszego OPZ

Zamawiający wymaga, aby suma MOCY OBLICZENIOWEJ serwerów w tej kategorii wynosiła dla każdej lokalizacji 332,8 Gflops lub więcej.

- Zamawiający wymaga, aby każdy z dostarczonych Zestawów Serwerowych Wariant C posiadał identyczną konfigurację i spełniał wymagania opisane w punkcie 13.3.3.1 niniejszego OPZ

#### 13.3.3.1 Serwer OBLICZENIOWY wariant C

Serwer obliczeniowy wariant C	
Parametr	Charakterystyka (wymagania minimalne)
SO C 1	Musi posiadać obudowę dedykowaną do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych o wielkości nie większej niż 2U.
SO C 2	<ul style="list-style-type: none"> <li>A. Wszystkie procesory Serwerów OBLICZENIOWYCH muszą być identyczne.</li> <li>B. Procesory muszą być typu x86, wykonywać instrukcje 64 bitowe oraz</li> </ul>

	<p>zawierać na sobie kontroler pamięci RAM.</p> <p>C. Zainstalowane co najmniej 2 procesory.</p> <p>D. Suma wydajności procesorów musi wynosić:</p> <ul style="list-style-type: none"> <li>i SPECint_base2006 <math>\geq</math> 49.8,</li> <li>ii SPECfp_base2006 <math>\geq</math> 79.7.</li> </ul> <p>B) Zamawiający wymaga, by dla zaoferowanego zestawu serwerów na stronie <a href="http://www.spec.org">www.spec.org</a> opublikowane były wyniki testów wydajności, potwierdzające spełnienie obu powyższych warunków dotyczących wydajności. Zamawiający dopuszcza, by wyniki te dotyczyły serwera innego producenta, serwera o innej konfiguracji lub innego modelu serwera niż oferowany serwer, pod warunkiem jednak, że serwer ten posiada taki sam zestaw procesorów co oferowany serwer.</p>
SO C 3	<p>A) Serwer musi posiadać 96 GB lub więcej pamięci RAM .</p> <p>B) Wszystkie moduły pamięci RAM wszystkich SERWERÓW muszą być identycznie między sobą.</p> <p>C) Serwer musi posiadać możliwość rozbudowy do co najmniej 384GB pamięci RAM dla każdego zainstalowanego procesora.</p> <p>D) Serwer musi posiadać pamięć z technologią ECC.</p>
SO C 4	<p>Serwer musi posiadać nadmiarowy, odporny na awarię 1 szt. zasilacza system, który spełnia następujące wymagania:</p> <ul style="list-style-type: none"> <li>A) Wymienny z zewnątrz, podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</li> <li>B) W ilości maksymalnej dla obudowy przewidzianej przez producenta obudowy.</li> </ul>
SO C 5	<p>Serwer musi posiadać nadmiarowy, odporny na awarię 1 szt. wentylatora system, który spełnia następujące wymagania:</p> <ul style="list-style-type: none"> <li>A) Wymienny podczas pracy obudowy, bez konieczności przerywania zadań wykonywanych przez serwery.</li> <li>B) W ilości maksymalnej dla obudowy przewidzianej przez producenta obudowy.</li> </ul>
SO C 6	Serwer musi posiadać co najmniej jeden napęd DVD-ROM
SO C 7	<p>Zamawiający wymaga by każdy SERWER posiadał niżej wyspecyfikowane porty. Zamawiający nie dopuszcza by jakiegokolwiek typ portu był przeznaczony do użycia w dwu lub więcej wymaganych standardach.</p> <p><u>standard SAS 6G:</u></p> <ul style="list-style-type: none"> <li>A) 1 para (2szt.) portów lub więcej par portów dokładnie SAS 6G.</li> <li>B) standard portów umożliwiający połączenie z SYSTEMEM ARCHIWIZACJI</li> </ul>

	<p>DANYCH wariant C opisanym poniżej.</p> <p><u>standard ETHERNET 1Gb</u></p> <p>A) 2 pary (4szt.) portów lub więcej par portów o przepustowości co najmniej 1Gb ETHERNET każdy.</p> <p>B) Wszystkie wymagane porty muszą być aktywne i umożliwiać połączenie do infrastruktury Zamawiającego.</p> <p>C) Każdy z portów musi posiadać wsparcie dla standardów: PXE oraz mechanizmów odciążenia procesora Large Send Offload (LSO), Segmentation Offload (TSO) oraz Cheksum Offload (CSO).</p> <p><u>standard USB/SD:</u></p> <p>A) 4 szt. portu lub więcej pracującego w standardzie USB lub SD.</p> <p>B) Co najmniej jeden z portów dostępny wewnątrz obudowy serwera.</p>
SO C 8	<p>Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na:</p> <p>A) włączenie, wyłączenie i restart serwera,</p> <p>B) podgląd logów sprzętowych serwera i karty,</p> <p>C) przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu i restartu OS),</p> <p>D) możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów.</p> <p>Rozwiązanie musi być niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.</p>

### 13.3.3.2 Zasób Dyskowy wariant C

Zamawiający wymaga dostarczenia co najmniej jednej sztuki (1 szt.) Zasobu Dyskowego wariant C dla każdego z oferowanych Serwerów Obliczeniowych Wariant C.

Ponadto każdy z oferowanych Zasobów dyskowych wariant C musi spełniać poniższe warunki:

Zasób Dyskowy wariant C	
Parametr	Charakterystyka (wymagania minimalne)
ZD C 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 4U.
ZD C 2	<p>Każdy oferowany zasób dyskowy musi udostępniać dwa rodzaje pojemności:</p> <p>A) Pojemność dyskowa dla danych produkcyjnych o sumarycznej wielkości 7,2 TB lub więcej w postaci 12 szt. lub więcej identycznych dysków twardych o parametrach:</p> <p>i Prędkość obrotowa 15.000 [RPM] o przepustowości minimum 6Gbit/s</p>

	<p>lub więcej z minimalnymi transferami 100 MB/s dla sekwencyjnego odczytu oraz 80 MB/s zapisu sekwencyjnego ALBO w technologii SSD z minimalnymi transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</p> <ul style="list-style-type: none"> <li>ii Wyposażony w 1 parę (2 szt.) portów SAS 6G / FC 8G. Awaria jednego portu z pary nie przerywa dostępu do danych znajdujących się na dysku.</li> <li>iii Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują.</li> </ul> <p>B) Pojemność dyskowa dla danych archiwizacji o sumarycznej wielkości 24 TB lub więcej w postaci 12 szt. lub więcej identycznych dysków twardych o parametrach:</p> <ul style="list-style-type: none"> <li>i Prędkość obrotowa 7.200 [RPM] o przepustowości minimum 6Gbit/s lub więcej ALBO w technologii SSD z minimalnymi transferami 200 MB/s dla sekwencyjnego odczytu oraz 100 MB/s zapisu sekwencyjnego.</li> <li>ii Dyski muszą być dostępne z zewnątrz urządzenia, w którym się znajdują oraz muszą być wymienne bez przerywania pracy i Serwera i urządzenia, w którym się znajdują.</li> <li>iii Musi istnieć możliwość rozbudowy Zasobu Dyskowego do co najmniej 200 Dysków Twardych w celu powiększenia przez Zamawiającego dostępnej pojemności dyskowej dla danych produkcyjnych ALBO pojemności dyskowej dla danych archiwizacji. Zaoferowany zasób dyskowy musi posiadać komplet licencji pozwalających na obsługę co najmniej 200 dysków twardych.</li> </ul>
ZD C 3	<p><u>Udostępnianie przestrzeni dyskowej</u> musi odbywać się przy wykorzystaniu:</p> <ul style="list-style-type: none"> <li>A) Co najmniej 1 pary (2 szt.) kontrolerów, każdy wyposażony w co najmniej 2 pary (4szt.) portów SAS 6G / FC 8G.</li> <li>B) Każdy z kontrolerów wyposażony w co najmniej 2 GB pamięci podręcznej, buforującej zapisy i odczyty. Pamięć nieulotna dostępna jednocześnie dla wszystkich zainstalowanych dysków twardych.</li> <li>C) Awaria jednego kontrolera z pary nie przerywa dostępu serwera do danych znajdujących się na dyskach Zasobu Dyskowego.</li> <li>D) Zamawiający wymaga, aby oferowany Zasób dyskowy miał możliwość rozbudowy do 8GB pamięci podręcznej Cache. Rozbudowa o dodatkową pamięć Cache musi być możliwa bez konieczności dokupowania dodatkowych licencji oraz z zachowaniem konfiguracji RAID, zachowaniem konfiguracji wszystkich dysków logicznych LUN oraz danych, które się na</li> </ul>

	nich znajdują.
ZD C 4	<p>Oferowany zasób dyskowy musi posiadać funkcjonalność:</p> <ul style="list-style-type: none"> <li>A) Tworzenia jednego z wybranych poziomów RAID 0,1,0+1,5,0+5,6 na wszystkich dostępnych dyskach twardych jednocześnie.</li> <li>B) Tworzenie Globalnego dysku spare.</li> <li>C) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</li> <li>D) Dynamiczną migrację danych z jednego typu dysków twardych na inny (np. z SAS na SATA), bez przerywania dostępu do danych serwerom.</li> <li>E) Możliwość rozbudowy Zasobu Dyskowego o funkcjonalność zdalnej replikacji danych (bez przerywania pracy systemu produkcyjnego) pomiędzy zaoferowanym Zasobem Dyskowym a Zasobem Dyskowym ZD-A znajdującym się w lokalizacji CPD opisanej poniżej. Zdalna replikacja musi odbywać się przy wykorzystaniu jedynie zasobów sprzętowych Zasobu Dyskowego w trybie synchronicznym jak i asynchronicznym. Rozbudowa o opisaną funkcjonalność zdalnej replikacji musi odbyć się poprzez instalację dodatkowych licencji, bez konieczności dokupowania dodatkowych elementów sprzętowych.</li> </ul>
ZD C 5	<p>Zarządzania za pomocą panelu GUI oraz CLI, o funkcjonalności co najmniej:</p> <ul style="list-style-type: none"> <li>A) Tworzenia poziomów RAID 0,1,1+0,5,5+0,6.</li> <li>B) Tworzenia/usuwania Globalnego dysku spare.</li> <li>C) Dynamiczną zmianę poziomu RAID bez przerywania dostępu do danych znajdujących się na dyskach.</li> <li>D) Dynamiczną zmianę wielkości wolumenów logicznych LUN, bez przerywania dostępu do danych znajdujących się na dyskach.</li> </ul>

### 13.3.3.3 System Archiwizacji DANYCH Wariant C

Zamawiający wymaga dostarczenia co najmniej jednej sztuki (1 szt.) Systemu Archiwizacji danych Wariant C dla każdego oferowanego serwera obliczeniowego wariant C składającego się na autoloader oraz oprogramowanie zarządzające tworzeniem kopii zapasowych.

Ponadto każdy z oferowanych Systemów Archiwizacji Danych wariant C musi spełniać poniższe warunki:

System Archiwizacji DANYCH Wariant C	
Parametr	Charakterystyka (wymagania minimalne)
SAD C 1	Obudowa dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, o wielkości nie większej niż 2U.



SAD C 2	Co najmniej 8 slotów przeznaczonych na zestaw taśm składających się z: A) 8 sztuk taśm w standardzie LTO5 lub lepszym o pojemności co najmniej 3 TB każda. B) 1 szt. taśmy czyszczącej. C) zestawu kodów kreskowych w celu identyfikacji każdej z dostarczonych taśm.
SAD C 3	Co najmniej 1 port SAS 6G w standardzie umożliwiającym połączenie do portu Serwera OBLICZENIOWEGO Wariant C opisanego w punkcie 13.3.3.1 niniejszego OPZ.
SAD C 4	Wyposażony w co najmniej 1 napęd o parametrach: A) standard LTO5 lub lepszy, B) przepustowość co najmniej 980GB/hr.

### 13.4 Dostawa i uruchomienie systemu zasilaczy bezprzerwowych (UPS)

Dostawa i uruchomienie zasilaczy bezprzerwowych (UPS)	
Parametr	Charakterystyka (wymagania minimalne)
DMO	Dostarczane zasilacze muszą spełniać niżej wyspecyfikowane wymagania:
DMO 1	Przystosowany do zamontowania w szafie rack 19" wraz z zestawem szyn montażowych oraz kompletem kabli zasilających o wysokości maksymalnie 2U.
DMO 2	A) Moc pozorna zasilacza powinna być nie mniejsza niż 3000VA B) Moc rzeczywista zasilacza powinna być nie mniejsza niż 3000W
DMO 3	A) Wymagany minimalny czas pracy z akumulatora nie może być krótszy niż 4 minut przy 100% obciążeniu oraz 12 minut przy obciążeniu równym 50%. B) Musi istnieć możliwość wydłużenia czasu pracy z akumulatora poprzez zastosowanie dodatkowych modułów akumulatorowych
DMO 4	Zasilacz powinien być wyposażony w: A) minimum 6 gniazd z utrzymaniem zasilania w standardzie IEC320 C13 (10A) B) minimum 2 gniazda z utrzymaniem zasilania w standardzie IEC320 C19 (16A).
DMO 5	Zasilacz powinien umożliwiać połączenie go do sieci ETHERNET oraz umożliwiać monitorowanie za pomocą protokołów SNMP oraz Telnet. Dopuszcza się, aby interfejs sieciowy był zainstalowany jako moduł.

### 13.5 Dostawa i uruchomienie komputerów osobistych

Celem realizacji projektu w zakresie dostawy i uruchomienia komputerów osobistych jest wyposażenie JST w komputery biurkowe i komputery przenośne zgodnie z zapotrzebowaniem określonym w Zał. nr 1.

Komputery te powinny być wyposażone w system operacyjny pakiet oprogramowania biurowego zawierający co najmniej: edytor tekstu, oprogramowanie do tworzenia arkuszy kalkulacyjnych, oprogramowanie do tworzenia prezentacji multimedialnych, oprogramowanie bazy danych, oprogramowanie antywirusowe oraz antymalware'owe wraz z subskrypcją na czas trwania gwarancji, aplikacja chroniąca przed atakami sieciowymi oraz personalny Firewall.

Wszystkie stacje mobilne powinny być wyposażone dodatkowo w klienta VPN: IPSec oraz SSL współpracującego z bramami VPN zainstalowanymi w poszczególnych lokalizacjach. Ponadto na stacjach mobilnych powinny być zainstalowane aplikacje kontroli treści WWW – zawierające ważne z punktu widzenia bezpieczeństwa kategorie jak: malware, spyware, phishing. W ramach postępowania powinny być dostarczone licencje na dostęp do serwerów kategorii stron na okres trwania gwarancji.

### **13.5.1 Komputery biurowe**

Komputery biurowe o parametrach nie gorszych, niż wyspecyfikowane w poniższej tabeli w kolumnie „Wymagane minimalne parametry techniczne komputerów”:

<b>Komputery biurowe</b>	
<b>Nazwa komponentu</b>	<b>Wymagane minimalne parametry techniczne komputerów</b>
KB 1	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
KB 2	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
KB 3	<p>A) Procesor klasy x86 wykonujący instrukcje 64bit, zaprojektowany do pracy w komputerach stacjonarnych.</p> <p>B) Komputer w oferowanej konfiguracji musi osiągać w teście BAPCo Sysmark2007 Preview ver. 1.06.1109 wyniki nie mniejsze niż:</p> <ul style="list-style-type: none"> <li>i Sysmark2007 Preview Rating – 278 pkt</li> <li>ii Sysmark2007 Preview - E-Learning – 253 pkt</li> <li>iii Sysmark2007 Preview - Video Creation – 322 pkt</li> </ul> <p>C) Test przeprowadzony przy ustawieniu „1. Only make changes that are REQUIRED In order for the benchmark to run” w programie konfiguracyjnym – Auto-Configuration Script.</p> <p>D) Test przeprowadzany dla jednokrotnego przebiegu (No. of Iterations=1) oraz z włączoną opcją „Perform Conditioning Run”,</p> <p>E) Test przeprowadzany na oferowanym zestawie komputerowym przy ustawionej rozdzielczości ekranu - 1280x1024@60Hz i jakości kolorów - najwyższa (32 bity).</p>

	<p>F) Wszystkie podzespoły oferowanego zestawu muszą pracować w zakresie parametrów ustawionych przez producenta danego podzespołu. Niedozwolony jest tzw. overclocking tj. podwyższenie częstotliwości taktowania procesora, karty graficznej, szyny systemowej lub jakiegokolwiek innego podzespołu ponad wartości ustawione przez jego producenta.</p> <p>G) Wykonawca składając ofertę zobowiązany dołączyć wydruk z wynikiem testów oferowanej konfiguracji. Test musi być potwierdzony przez producenta sprzętu (lub jego przedstawiciela w Polsce).</p> <p>H) Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może być wezwany do dostarczenia Zamawiającemu licencjonowanego oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu w celu ich sprawdzenia, w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.</p>
KB 4	8GB (1x8096MB lub 2x4096MB) prędkość transferu min 12 GB/s, możliwość rozbudowy do min 16GB, min. jeden slot wolny.
KB 5	Min. 320 GB SATA III (min. prędkość transferu 100 MB/s dla sekwencyjnego odczytu oraz 50 MB/s zapisu sekwencyjnego)
KB 6	Zestaw powinien umożliwiać pracę dwu-monitorową o rozdzielczości nominalnej 1920x1080 @ 60Hz (cyfrowo) i 1920x1080 @ 75Hz (analogowo), wspierać technologię DirectX w wersji 11, OpenGL w wersji 3.0 i Shader 5.0.
KB 7	Min 24-bitowa karta dźwiękowa zintegrowana z płytą główną, Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
KB 8	<p>Obudowa:</p> <p>A) Typu desktop, umożliwiająca pracę w pionie jak i w poziomie, z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w min. 3 kieszenie: 1 szt 5,25" zewnętrzne i 2szt 3,5" wewnętrzne.</p> <p>B) Obudowa powinna fabrycznie umożliwiać montaż min 2 szt. dysków 3,5" lub 2,5".</p> <p>C) Suma wymiarów obudowy nie może przekraczać 100 cm. Zasilacz o mocy max 300W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85%.</p> <p>D) Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i 3,5" dysku twardego bez konieczności użycia narzędzi.</p> <p>E) Obudowa w jednostce centralnej musi być otwierana bez</p>

	<p>konieczności użycia narzędzi oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzającym – diagnostycznym producenta komputera.</p> <p>F) Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki).</p> <p>G) Obudowa musi być wyposażona w zamek, który nie wystaje poza obrys obudowy.</p> <p>H) Obudowa musi posiadać wbudowany wizualny lub dźwiękowy system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować:</p> <ul style="list-style-type: none"> <li>i uszkodzenie lub brak pamięci RAM,</li> <li>ii uszkodzenie złączy PCI i PCIe, płyty głównej,</li> <li>iii uszkodzenie kontrolera Video,</li> <li>iv uszkodzenie dysku twardego,</li> <li>v awarię BIOS'u,</li> <li>vi awarię procesora.</li> </ul> <p>I) Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w OPZ</p>
KB 9	<p>Wymagany system operacyjny Windows 7 lub równoważny. System równoważny powinien posiadać następujące cechy:</p> <ul style="list-style-type: none"> <li>A) wsparcie dla architektury 32 i 64 bitowej,</li> <li>B) obsługa procesorów wielordzeniowych,</li> <li>C) graficzny okienkowy interfejs użytkownika,</li> <li>D) obsługa co najmniej 8 GB RAM,</li> <li>E) pełna obsługa sprzętu będącego przedmiotem zamówienia (kompatybilność sterowników, w tym sterowników do urządzeń peryferyjnych),</li> <li>F) współpraca z zamawianym pakietem biurowym,</li> <li>G) współpraca z Active Directory, możliwość pracy sieciowej,</li> <li>H) możliwość darmowej aktualizacji poprzez sieć,</li> <li>I) posiadający wsparcie pomocy technicznej producenta co najmniej do końca 2014 roku.</li> </ul> <p>Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 32bit i 64bit (załączyć wydruk ze strony</p>

	Microsoft WHCL).
KB 10	<p>A) Komputer musi posiadać zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego do zaszyfrowania całości dysku, przy czym wszystkie dane muszą być dostępne, kiedy system operacyjny działa.</p> <p>B) Komputer musi być zaopatrzony w etykietę inwentaryzacyjną umieszczoną przez producenta sprzętu zawierającą informacje:</p> <ul style="list-style-type: none"> <li>i numer ewidencyjny produktu,</li> <li>ii oznaczenie modelu wg nazewnictwa producenta.</li> </ul> <p>C) Oprogramowanie zainstalowane przez producenta komputera umożliwiające wygenerowanie raportu środków trwałych raz w tygodniu bez konieczności dokonywania spisu lokalnie lub zdalnie. Wygenerowany raport musi zawierać:</p> <ul style="list-style-type: none"> <li>i numer seryjny komputera,</li> <li>ii informacje o typie i pojemności zainstalowanego dysku HDD,</li> <li>iii informacje o zainstalowanym systemie,</li> <li>iv informacje o MAC adresie karty sieciowej,</li> <li>v informacje o zainstalowanym procesorze,</li> <li>vi informacje o zainstalowanej pamięci operacyjnej RAM,</li> <li>vii informacje o typie zainstalowanej karcie graficznej,</li> <li>viii informacje o zainstalowanej karcie muzycznej,</li> </ul> <p>D) Zainstalowane oprogramowanie musi umożliwiać generowanie raportu do pliku .xls.</p>
KB 11	<p>Komputer musi posiadać wbudowaną w płytę główną technologię zarządzania i monitorowania komputerem na poziomie sprzętowym, działającą niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniającą:</p> <ul style="list-style-type: none"> <li>A) monitorowanie konfiguracji komponentów komputera – CPU, Pamięć, HDD wersja BIOS płyty głównej,</li> <li>B) zdalną konfigurację ustawień BIOS,</li> <li>C) zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD</li> </ul>

	<p>z serwera zarządzającego,</p> <p>D) zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie,</p> <p>E) zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.</p> <p>F) technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (<a href="http://www.dmtf.org/standards/wsman">http://www.dmtf.org/standards/wsman</a>) oraz DASH 1.0.0 (<a href="http://www.dmtf.org/standards/mgmt/dash/">http://www.dmtf.org/standards/mgmt/dash/</a>),</p> <p>G) nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS.</p> <p>H) wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego</p> <p>I) sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji</p> <p>J) automatyczne rozpoznawanie obrotu ekranu z odpowiednią kalibracją pulpitu</p> <p>K) obsługa zdalnego podłączenia do 3 wyświetlaczy.</p>
KB 12	Komputer musi posiadać sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
KB 13	<p>Komputer musi posiadać</p> <p>A) BIOS zgodny ze specyfikacją UEFI.</p> <p>B) Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p>

	<ul style="list-style-type: none"> <li>i wersji BIOS,</li> <li>ii ilości RAM,</li> <li>iii typie procesora,</li> <li>iv pojemności zainstalowanego dysku twardego,</li> <li>v rodzajach napędów optycznych,</li> <li>vi MAC adresie zintegrowanej karty sieciowej,</li> <li>vii kontrolerze audio.</li> </ul> <p>C) Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS).</p> <p>D) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznymi urządzeniami.</p> <p>E) Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora.</p> <p>F) Możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.</p> <p>G) Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p> <p>H) Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.</p>
KB 14	<p>Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej:</p> <p>A) Informowanie administratora o otwarciu obudowy.</p>

	<p>B) Zdalne zablokowanie stacji dysków, portów szeregowych, równoległych, USB.</p> <p>C) Zdalne uaktualnianie BIOS zarówno na pojedynczym komputerze a także na grupie komputerów w tym samym czasie.</p> <p>D) Zdalną konfigurację BIOS w czasie rzeczywistym, w tym co najmniej ustawienie hasła, wpisanie unikalnego numeru nadanego przez użytkownika, sekwencji startowej, włączenia/wyłączenia portów USB, włączenia/wyłączenia karty dźwiękowej.</p> <p>E) Zdalne wyłączenie oraz restart komputera w sieci.</p> <p>F) Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS.</p> <p>G) Monitorowanie i alertowanie parametrów termicznych, wolnego miejsca na dyskach twardych.</p> <p>H) Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS przy wyłączonym komputerze lub nieobecnym/uszkodzonym systemie operacyjnym.</p> <p>I) Zdalne przejęcie konsoli tekstowej stacji roboczej przy wyłączonym komputerze lub nieobecnym/uszkodzonym systemie operacyjnym.</p> <p>Oprogramowanie musi umożliwiać ustawienie sposobu informowania o zaistnieniu zdarzenia poprzez (po stronie serwera) automatyczne uruchomienie zaplanowanej wcześniej akcji, wysłanie raportu zawierającego między innymi numer seryjny komputera i opis błędu na wskazany adres poczty elektronicznej.</p>
KB 15	<p>Oferowane modele komputerów muszą posiadać:</p> <p>A) certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty).</p> <p>B) certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 32bit i 64bit (załączyć wydruk ze strony Microsoft WHCL).</p> <p>C) Deklaracja zgodności CE (załączyć do oferty).</p> <p>D) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „<i>Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych</i>”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych</p>



	<p>z tworzyw sztucznych o masie powyżej 25 gram.</p> <p>E) Komputer musi spełniać wymogi normy Energy Star 5.0.</p> <p>F) Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu <a href="http://www.eu-energystar.org">http://www.eu-energystar.org</a> lub <a href="http://www.energystar.gov">http://www.energystar.gov</a> – (Zamawiający wymaga przedłożenia wraz ofertą wydruku ze strony internetowej, zaświadczenia lub certyfikatu).</p>
KB 16	<p>Musi być zapewniona możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.</p>
KB 17	<p>Komputer mus posiadać:</p> <p>A) Zainstalowany system operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie producenta oprogramowania + nośnik.</p> <p>B) Wbudowane porty (minimum dwa) umożliwiające podłączenie zewnętrznego monitora w standardzie:</p> <ul style="list-style-type: none"> <li>i D-SUB (analogowy VGA)</li> <li>ii DVI-D</li> </ul> <p>C) min. 8 portów USB wyprowadzonych na zewnątrz komputera w tym min 3 porty USB 3.0; min. 2 porty USB muszą znajdować się z przodu obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.,</p> <p>D) porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.</p> <p>E) Kartę sieciową 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1, umożliwiającą zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania - niezależnie od stanu zasilania komputera – łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie).</p> <p>F) Płytę główną zaprojektowaną i wyprodukowaną na zlecenie producenta komputera, dedykowana dla danego urządzenia; wyposażona w: min 2 złącza PCI Express x16 w tym jedno elektrycznie</p>

	<p>jak PCIe x4, min. jeden wolny slot PCI Express; min. jedno wolne złącze PCI 32bit, min. 4 złącza DIMM z obsługą do 16GB pamięci RAM, min. 3 złącza SATA w tym 2 szt. SATA 3.0;.</p> <p>G) Klawiaturę USB w układzie QWERTY obsługującą standard polski programisty.</p> <p>H) Mysz optyczną USB z trzema klawiszami oraz rolką (scroll).</p> <p>I) Nagrywarke DVD +/-RW DL wraz z oprogramowaniem do nagrywania i odtwarzania płyt.</p> <p>J) Dołączony nośnik ze sterownikami.</p> <p>K) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.</p>
--	--

### 13.5.2 Monitor ciekłokrystaliczny

Monitory ciekłokrystaliczne o parametrach nie gorszych (t.j. nie przekraczających wartości określonych jako maksymalne, ani nie mniejszych od wartości określonych jako minimalne), niż wyspecyfikowane w poniższej tabeli w kolumnie „Wymagane minimalne parametry techniczne monitora”:

Monitor ciekłokrystaliczny	
Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
MC 1	Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą TFT 22"
MC 2	Rozmiar plamki: 0,282 mm
MC 3	Jasność: 250 cd/m <sup>2</sup>
MC 4	Kontrast: Typowy 1000:1
MC 5	Kąty widzenia (pion/poziom): 160° w pionie/170° w poziomie
MC 6	Czas reakcji matrycy: max 5ms (od czerni do bieli)
MC 7	Rozdzielczość nominalna: co najmniej 1920x 1080 przy 60Hz
MC 8	Częstotliwość odświeżania poziomego: 30 – 80 kHz
MC 9	Częstotliwość odświeżania pionowego: 56 – 75 Hz
MC 10	Nachylenie monitora: w zakresie -4 do +15 stopni
MC 11	Zużycie energii typowo 35W, maksymalnie 45W
MC 12	Powłoka powierzchni ekranu: antyodblaskowa
MC 13	Podświetlenie: system podświetlenia LED
MC 14	Bezpieczeństwo: monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.
MC 15	Złącze: 15-stykowe złącze D-Sub, złącze DVI-D

MC 16	Certyfikaty: TCO 5, ISO 13406-2 lub ISO 9241, Energy Star 5.0
MC 17	<p>Inne:</p> <p>A) Monitor i zestaw centralny muszą być objęte jednakowym poziomem serwisu z jednym punktem kontaktowym dla całego zestawu.</p> <p>B) Monitor musi posiadać trwałe oznaczenie logo producenta.</p> <p>C) Zdemowana podstawa oraz otwory montażowe w obudowie VESA 100mm.</p> <p>D) Głośniki w obudowie monitora min. 2x1W.</p>

### 13.5.3 Komputery przenośne – „notebook”

Wykonawca musi dostarczyć komputery przenośne o parametrach nie gorszych, niż wyspecyfikowane w poniższej tabeli w kolumnie „Wymagane minimalne parametry techniczne komputerów”:

<b>Komputery przenośne – „notebook”</b>	
<b>Nazwa komponentu</b>	<b>Wymagane minimalne parametry techniczne komputerów</b>
KP 1	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości: HD (1366x768) w technologii LED przeciwoodblaskowy,.
KP 2	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
KP 3	<p>Procesor klasy x86, procesor wielordzeniowy, zaprojektowany do pracy w komputerach przenośnych, z pamięcią lastlevel cache CPU, co najmniej 3 MB lub równoważny wielordzeniowy procesor klasy x86wykonujący instrukcje 64bit.</p> <p>Zaoferowany procesor musi uzyskiwać jednocześnie w teście MobileMark 2007 Runtime (scenari: productivity 2007) min 633 pkt. wynik tylko dla procesora.</p> <p>W przypadku użycia przez oferenta testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.</p>
KP 4	Pamięć operacyjna RAM 4GB (2x2048MB) prędkość transferu min 12 GB/smożliwość rozbudowy do min 8GB.
KP 5	Parametry pamięci masowej:Min. 120GB SSDlub 320 GB SATA.

KP 6	<p><u>Karta graficzna</u></p> <p>Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, obsługująca min. 2 monitory ze sprzętowym wsparciem dla DirectX 11, Shader 5.0 Posiadająca min. 16EU (Graphics ExecutionUnits) oraz Dual HD HW Decode, OPEN GL 3.X.</p>
KP 7	<p>Wyposażenie multimedialne: Karta dźwiękowa zgodna z HD, wbudowane głośniki.</p>
KP 8	<p><u>Zasilanie i akumulator:</u></p> <p>A) 6-cell, 60Whr, Li-Ion.</p> <p>B) Możliwość zwiększenia efektywnej pojemności akumulatora bądź przez zainstalowanie dodatkowego akumulatora 3-cell (30Whr) bądź przez zainstalowanie jednego większego akumulatora 90 Whr – Wykonawca przedstawi oświadczenie producenta o takiej możliwości.</p> <p>C) Zasilacz o mocy min. 65W.</p>
KP 9	<p><u>Zdalne zarządzanie</u></p> <p>Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:</p> <p>A) monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej,</p> <p>B) zdalną konfigurację ustawień BIOS,</p> <p>C) zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego,</p> <p>D) zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie,</p> <p>E) zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej,</p> <p>F) technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF</p>

	<p>WS-MAN 1.0.0 (<a href="http://www.dmtf.org/standards/wsman">http://www.dmtf.org/standards/wsman</a>) oraz DASH 1.0.0 (<a href="http://www.dmtf.org/standards/mgmt/dash/">http://www.dmtf.org/standards/mgmt/dash/</a>),</p> <p>G) nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS.</p> <p>H) wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego,</p> <p>I) sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji,</p> <p>J) automatyczne rozpoznawanie obrotu ekranu z odpowiednią kalibracją pulpitu,</p> <p>K) obsługa zdalnego podłączenia do 3 wyświetlaczy.</p>
KP 10	<p>Komputer przenośny musi posiadać sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).</p>
KP 11	<p><u>Komputer przenośny musi posiadać:</u></p> <p>A) BIOS zgodny ze specyfikacją UEFI.</p> <p>B) Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> <li>i wersji BIOS,</li> <li>ii ilości i sposobu obciążenia slotów pamięciami RAM,</li> <li>iii typie procesora,</li> <li>iv pojemności zainstalowanego dysku twardego,</li> <li>v rodzaju napędu optycznego,</li> <li>vi MAC adresie zintegrowanej karty sieciowej,</li> <li>vii zainstalowanej grafice.</li> </ul> <p>C) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.</p> <p>D) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej</p>

	<p>z USB.</p> <p>E) Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora.</p> <p>F) Możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.</p> <p>G) Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, portów USB, portu eSATA, modemu analogowego, wnęki na napęd optyczny, czytnika kart multimedialnych, mikrofonu, kamery, systemu ochrony dysku przed upadkiem, ASF 2.0, pracy wielordzeniowej procesora, modułów: WWAN, WLAN i Bluetooth z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p>
KP 12	<p><u>Komputer przenośny musi posiadać</u></p> <p>A) Zamawiający wymaga dołączenia do oferty dokumentów poświadczających, że komputer przenośny jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 Komputer przenośny musi posiadać Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty).</p> <p>B) Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty).</p> <p>C) Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 7 32bit/64bit (załączyć wydruk ze strony Microsoft WHCL).</p> <p>D) Deklaracja zgodności CE (załączyć do oferty).</p> <p>E) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.</p> <p>F) Certyfikat EnergyStar 5.0 – Komputer musi znajdować się na liście zgodności dostępnej na stronie</p>

	<a href="http://www.energystar.gov">www.energystar.gov</a> oraz <a href="http://www.eu-energystar.org">http://www.eu-energystar.org</a> .
KP 13	<p><u>Komputer przenośny musi posiadać następujące parametry:</u></p> <p>A) Waga max 2.8 kg z akumulatorem</p> <p>B) Szerokość: max 384 mm</p> <p>C) Wysokość: max 35 mm</p> <p>D) Głębokość: max 258 mm</p>
KP 14	<p><u>Bezpieczeństwo</u></p> <p>A) Komputer przenośny musi posiadać zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.</p> <p>B) Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.</p> <p>C) Komputer przenośny musi posiadać czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy</p> <p>D) Komputer przenośny musi posiadać złącze typu Kensington Lock</p> <p>E) Komputer przenośny musi być zaopatrzony w etykietę Inwentaryzacyjną umieszczoną przez producenta sprzętu zawierającą informacje:</p> <ul style="list-style-type: none"> <li>i informacje o zainstalowanym procesorze,</li> <li>ii numer ewidencyjny produktu,</li> <li>iii oznaczenie modelu wg nazewnictwa producenta,</li> <li>iv informacje o zainstalowanym systemie operacyjnym.</li> </ul>
KP 15	<p><u>Wymagania dodatkowe</u></p> <p>Komputer przenośny musi posiadać:</p> <p>A) wbudowane porty i złącza: 1xVGA, 1 x HDMI/DisplayPort, 4 szt. USB w tym 1 szt o funkcjonalności eSATA oraz w tym min. 2 szt. 3.0 i jedno dosilone, RJ-45, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, czytnik kart multimedialnych(czytający min. Hi Density oraz Hi Capacity SD / SD-XC / SD Legacy / SDIO / MMC / MS, MS Pro), możliwość podłączenia dedykowanego replikatora portów niezaajmującego złącza USB, wbudowana kamera 1,2 Mpix w obudowę ekranu komputera, mikrofon z funkcjami redukcji szumów i poprawy mowy,</p>

	<p>B) Kartę sieciową LAN 10/100/1000 Ethernet RJ 45 zintegrowaną z płytą główną oraz WLAN 802.11N, zintegrowany z płytą główną lub w postaci wewnętrznego modułu mini-PCI Express z dedykowanym przełącznikiem do uruchamiania modułu WLAN.</p> <p>Obie sieci LAN i WLAN muszą umożliwiać zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania- niezależnie od stanu zasilania komputera – przy pracy na zasilaczu - łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie).</p> <p>C) Klawiaturę (układ US -QWERTY), min 102 klawisze z wydzieloną z prawej strony klawiaturą numeryczną Touchpad 240 CPI ze strefą przewijania w pionie i w poziomie wraz z obsługą gestów.</p> <p>D) Wbudowany moduł Bluetooth 4.0.</p> <p>E) Wbudowany moduł HSDPA.</p> <p>F) Replikator portów.</p> <p>G) Napęd optyczny 8x DVD +/- RW wewnętrzny w modułowej kieszeni z możliwością zapisu i odczytu w technologii DL.</p> <p>H) Dołączone oprogramowanie do nagrywania i odtwarzania.</p> <p>I) Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>J) Dołączony nośnik ze sterownikami.</p> <p>K) Kąt otwarcia notebooka min 140 stopni.</p> <p>L) Szkielet i obudowa notebooka wzmacniane, wykonane z metalu.</p> <p>M) Kieszeń modułarna musi mieć możliwość obsługi: urządzeń optycznych, dodatkowego dysku twardego i dodatkowego akumulatora.</p> <p>N) Zestaw wyposażony w dodatkową klawiaturę oraz mysz bezprzewodową.</p> <p>O) System operacyjny Windows 7 lub równoważny. System równoważny powinien posiadać następujące cechy:</p> <ul style="list-style-type: none"> <li>i wsparcie dla architektury 32 i 64 bitowej,</li> <li>ii obsługa procesorów wielordzeniowych,</li> <li>iii graficzny okienkowy interfejs użytkownika,</li> <li>iv obsługa co najmniej 8 GB RAM,</li> </ul>
--	--



	<ul style="list-style-type: none"> <li>v pełna obsługa sprzętu będącego przedmiotem zamówienia (kompatybilność sterowników, w tym sterowników do urządzeń peryferyjnych),</li> <li>vi współpraca z zamawianym pakietem biurowym,</li> <li>vii współpraca z Active Directory, możliwość pracy sieciowej,</li> <li>viii możliwość darmowej aktualizacji poprzez sieć,</li> <li>ix posiadający wsparcie pomocy technicznej producenta co najmniej do końca 2014 roku.</li> </ul>
--	---

### 13.6 Zestawy do podpisu elektronicznego

Zamawiający oczekuje dostawy zestawów kwalifikowanego podpisu elektronicznego, składających się z czytnika i karty-nośnika podpisu oraz odpowiedniego oprogramowania. Zamawiający wymaga w ramach zakupu opłaty za odnawianie podpisu na okres 5 lat.

Zestawy do podpisu elektronicznego	
Wymaganie	Minimalne wymagania dotyczące centrum certyfikacji
PECC 1	Świadczenie usługi wystawiania kwalifikowanych certyfikatów zgodnie z ustawą o Podpisie Elektronicznym.
PECC 2	Świadczenie usługi kwalifikowanych znaczników czasu.
PECC 3	Świadczenie usługi weryfikacji stanu certyfikatu online.
PECC 4	Możliwość wystawienia certyfikatu w siedzibie klienta.
PECC 5	Możliwość wystawienia certyfikatu w czasie poniżej 15 minut.
PECC 6	Możliwość wystawienia certyfikatu do 2048 bitowych kluczy.
PECC 7	Darmowy dzienny pakiet znaczników czasu (co najmniej 700 znaczników w okresie 5 lat).
PECC 8	Świadczenie usług całodobowego wsparcia technicznego.
PECC 9	Świadczenie usługi bezpłatnej aktualizacji oprogramowania służącego do składania podpisu cyfrowego.
PECC 10	Świadczenie usługi instalacji certyfikatu i krótkie szkolenie z funkcjonalności wykonania podpisu w siedzibie klienta.

<b>Zestawy do podpisu elektronicznego</b>	
<b>Wymaganie</b>	<b>Minimalne wymagania dotyczące karty (nośnika)</b>
PEKA 1	Karty z interfejsem stykowym według standardu ID-1 (zgodne ze standardem ISO 7816-1,2,3,4,8).
PEKA 2	Obsługa funkcji skrótu przynajmniej SHA-1 i SHA-256.
PEKA 3	Obsługą algorytmów przynajmniej DES, 3DES.
PEKA 4	Karty posiadają certyfikat bezpieczeństwa dla układu z interfejsem stykowym spełniające wymagania dla komponentu technicznego w rozporządzeniach do Ustawy o podpisie elektronicznym z dnia 18 września 2001r.
PEKA 5	Możliwość ustawienie różnych kodów PIN dla co najmniej 5 kluczy prywatnych.
PEKA 6	Możliwość zarządzania kluczami, certyfikatami i obiektami danych na karcie.
PEKA 7	Możliwość ustawienie kodu PIN o długości 4-64 znaki zapisane w standardzie UTF-8.

<b>Zestawy do podpisu elektronicznego</b>	
<b>Wymaganie</b>	<b>Minimalne wymagania oprogramowania</b>
PEOP 1	Możliwość weryfikacji stanu certyfikatu służącego do weryfikacji podpisu elektronicznego online.
PEOP 2	Możliwość składania podpisu w formatach: CAdES, XAdES, PAdES.
PEOP 3	Możliwość wykonywania postaci archiwalnej podpisu.
PEOP 4	Aplikacja powinna działać pod następującymi systemami operacyjnymi: Windows 2000/XP/2003/2008/Vista/7, Mac OS X 10.6, Ubuntu 10.10 32 bit (GNOME 2.32.0, KDE 4.5.1 + Qt 4.7.0).
PEOP 5	Aplikacja może współpracować z serwerami proxy.
PEOP 6	Aplikacja pozwala na zapamiętywanie kodu PIN na zadany okres czasu.
PEOP 7	Aplikacji automatycznie weryfikuje dostępność aktualizacji i informuje o tym użytkownika.

## 13.7 Dostawa i uruchomienie infomatów

Celem realizacji projektu w zakresie dostawy i uruchomienia infomatów jest wyposażenie Zamawiającego w nowoczesne urządzenia typu kiosk internetowy, przeznaczone do wykorzystania przez mieszkańców w charakterze publicznych punktów dostępu do Internetu oraz jako multimedialna witryna JST.

### 13.7.1 Obudowa infomatu wewnętrznego

Obudowa infomatu wewnętrznego	
Wymaganie	Minimalne wymagania dotyczące Obudowy infomatu wewnętrznego
OIW 1	<p>A) Obudowa infomatu wewnętrznego musi stanowić spójną konstrukcję, w której wyróżnić można dwie zasadnicze części: korpus z podstawą i obudowę monitora dotykowego. Obudowa infomatu wewnętrznego musi być:</p> <ul style="list-style-type: none"> <li>i wolnostojąca,</li> <li>ii dużej odporności na uszkodzenia mechaniczne,</li> <li>iii naturalnie stabilna, bez potrzeby kotwienia.</li> </ul> <p>B) Wszystkie wymienione części (obudowa monitora, korpus z podstawą) muszą być ze sobą trwale połączone, zapewniając sztywność całej konstrukcji.</p> <p>C) Nie dopuszcza się stosowania zewnętrznych materiałów wykończeniowych innych niż stal malowana proszkowo, laminat oraz lakierowany MDF.</p>
OIW 2	Część, w której jest zabudowany monitor, musi zapewniać możliwość korzystania z infomatu przez osoby poruszające się na wózkach inwalidzkich. Przyjmuje się, że elementy do odczytu i wprowadzania danych muszą być w takiej sytuacji dostępne na wysokości 0,9 – 1,1 m od poziomu posadzki, przy czym najwyższy zasięg osoby siedzącej na wózku jest nie wyższy niż 1,4 m.
OIW 3	Korpus musi być przystosowany do zamontowania jednostki komputerowej oraz listwy elektrycznej, przy jednoczesnym zapewnieniu sprawnej wentylacji zabudowanych wewnątrz urządzeń.
OIW 4	Nie dopuszcza się występowania szczelin w miejscach styczności nakładki dotykowej monitora i obudowy, przy czym nie dopuszcza się również stosowania wypełniających uszczelniaczy (jak np. silikon).
OIW 5	Technologia wykonania obudowy musi zapewniać brak widocznych i dostępnych śrub, gwintów, nitów w korpusie infomatu i obudowie monitora dotykowego.
OIW 6	Konstrukcja obudowy musi zapewniać brak zewnętrznego dostępu do kabli

	związanych z instalacją wewnętrzną infomatu.
OIW 7	Obudowa malowana proszkowo farbą poliestrową, drobnostrukturową w kolorach wybranych przez Zamawiającego z palety RAL. Przyjmuje się, iż do wszystkich lokalizacji będą dostarczane obudowy w jednym wybranym przez Zamawiającego kolorze.

### 13.7.2 Jednostka komputerowa infomatu wewnętrznego

Wymagania minimalne dotyczące parametrów jednostki komputerowej infomatu wewnętrznego zostały przedstawione w poniższej tabeli:

<b>Jednostka komputerowa infomatu wewnętrznego</b>	
<b>Nazwa komponentu</b>	<b>Minimalne wymagania dotyczące Jednostki komputerowej infomatu wewnętrznego</b>
JKIW	Jednostka komputerowa infomatu wewnętrznego musi posiadać poniższe parametry:
JKIW 1	Procesor wielordzeniowy, dedykowany do pracy w komputerach stacjonarnych, w architekturze x64 o wydajności min 235 pkt w teście SYSmark 2007 Preview Rating – wydruk dołączony do testów.
JKIW 2	Pamięć RAM: A) 2GB prędkość transferu min 12 GB/s, B) możliwość rozbudowy do 16 GB, C) min. 2 wolne złącza dla rozszerzeń pamięci.
JKIW 3	Dysk twardy: 320GB (min. prędkość transferu 100 MB/s dla sekwencyjnego odczytu oraz 50 MB/s zapisu sekwencyjnego)
JKIW 4	Napęd optyczny: DVD-RW SATA z oprogramowaniem do odtwarzania i nagrywania płyt DVD, napęd slot-in (brak wysuwanej tacki lub innych wystających elementów konstrukcyjnych, które mogą ulec uszkodzeniu przy nieuważnym użytkowaniu), sprzętowy przycisk wysuwania nośnika optycznego na przedniej ścianie urządzenia.
JKIW 5	Płyta główna zaprojektowana i wyprodukowana przez producenta komputera A) logo producenta, model płyty oraz numer katalogowy trwale naniesiony na powierzchnię na etapie produkcji, B) obsługa procesorów wielordzeniowych wspierających wirtualizację, C) zintegrowany kontroler 3 x SATA, D) min 1x PCI -Express 2.0 x16 (low profile), E) możliwość zabezpieczenia hasłem dostępu do systemu operacyjnego i dostępu do BIOS komputera - zabezpieczenia te muszą działać

	<p>niezależnie od siebie,</p> <p>F) możliwość zabezpieczenia dysku twardego w sposób uniemożliwiający możliwość odczytu danych po podłączeniu dysku do innego komputera,</p> <p>G) możliwość odczytania z BIOS komputera informacji o numerze seryjnym, numerze inwentaryzacyjnym,</p> <p>H) możliwość odczytania z BIOS dokładnych informacji o procesorze – co najmniej model, typ, częstotliwości pracy,</p> <p>I) możliwość odczytania bezpośrednio z BIOS informacji o wersji i dacie wydania używanej wersji BIOS,</p> <p>J) możliwość sprawdzenia z poziomu BIOS modelu i wersji firmware dysku twardego oraz modelu i wersji firmware napędu optycznego,</p> <p>K) możliwość przekierowania konsoli tekstowej oraz ekranu konfiguracyjnego BIOS na stację zarządzającą przez sieć LAN,</p> <p>L) wbudowany firewall sprzętowy działający niezależnie od obecności systemu operacyjnego, zarządzany i konfigurowalny zdalnie, nie widoczny dla systemu operacyjnego czy aplikacji.</p>
JKIW 6	<p><u>Karta dźwiękowa:</u></p> <p>A) zintegrowana, w standardzie High Definition,</p> <p>B) możliwość wyłączenia karty muzycznej w BIOS.</p>
JKIW 7	<p><u>Karta sieciowa</u></p> <p>A) 10/100/1000 MBit/s,</p> <p>B) obsługa protokołów: WoL, ASF 2.0, PXE 2.1,</p> <p>C) możliwość wyłączenia karty sieciowej w BIOS,</p> <p>D) możliwość odczytania adresu MAC karty z BIOS komputera.</p>
JKIW 8	<p><u>Karta graficzna</u></p> <p>Zintegrowana, z możliwością dynamicznego przydzielania pamięci w obrębie pamięci systemowej, ze wsparciem dla DirectX 10.1, HDCP i OpenGL 2.1, np. Intel HD Graphics lub równoważna, możliwość pracy na dwóch ekranach jednocześnie, 1x DVI-D.</p>
JKIW 9	<p><u>Porty I/O</u></p> <p>A) min. 12 portów USB (w tym min. 3 porty USB 3.0) zintegrowanych trwale w komputerze (w tym min. 4 na panelu przednim)</p> <p>B) min. 1x porty szeregowy,</p> <p>C) 1x wyjście słuchawkowe oraz 1x wejście mikrofonowe na panelu przednim obudowy,</p> <p>D) 1x DVI,</p>

	E) dopuszcza się możliwość zastąpienia złączy USB znajdujących się na panelu przednim elastycznymi zaślepkami na pojedyncze złącza USB.
JKIW 10	<p>System operacyjny Windows Embedded POSReady 7 lub równoważny.</p> <p>System równoważny powinien posiadać następujące cechy:</p> <ul style="list-style-type: none"> <li>A) wsparcie dla architektury 32 i 64 bitowej,</li> <li>B) obsługa procesorów wielordzeniowych,</li> <li>C) graficzny okienkowy interfejs użytkownika,</li> <li>D) obsługa co najmniej 8 GB RAM,</li> <li>E) pełna obsługa sprzętu będącego przedmiotem zamówienia (kompatybilność sterowników, w tym sterowników do urządzeń peryferyjnych),</li> <li>F) współpraca z Active Directory, możliwość pracy sieciowej,</li> <li>G) możliwość darmowej aktualizacji poprzez sieć,</li> <li>H) posiadający wsparcie pomocy technicznej producenta co najmniej do końca 2015 roku.</li> </ul>
JKIW 11	<p>Obudowa:</p> <ul style="list-style-type: none"> <li>A) małogabarytowa,</li> <li>B) fabrycznie przystosowana do pracy w pionie i w poziomie,</li> <li>C) malowana proszkowo farbą poliestrową, droбноstrukturową w kolorach wybranych przez Zamawiającego z palety RAL. Przyjmuje się, iż do wszystkich lokalizacji będą dostarczane obudowy w jednym wybranym przez Zamawiającego kolorze.</li> <li>D) zasilacz o mocy nieprzekraczającej 300W,</li> <li>E) zasilacz z aktywnym filtrem PFC o sprawności minimum 80% przy pełnym obciążeniu komputera,</li> <li>F) obudowa zapewniająca możliwość beznarzędziowej obsługi w zakresie otwarcia obudowy (nie dopuszcza się żadnego rodzaju śrub w tym np. motylkowych), wymiany i instalacji kart rozszerzeń i dysków twardych (możliwość interwencyjnego, szybkiego zabezpieczenia przez użytkownika dysku twardego) bez konieczności użycia narzędzi,</li> <li>G) suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie więcej niż 670mm w tym głębokość nie więcej niż 315mm,</li> <li>H) licencja na system operacyjny oraz numer seryjny komputera umieszczony na górnej części obudowy,</li> <li>I) slot Kensington,</li> <li>J) obudowa musi posiadać czujnik otwarcia obudowy wraz z logowaniem</li> </ul>

	<p>otwarcia, współpracujący z dostarczoną aplikacją zarządzającą, wyklucza się zastosowanie czujników zajmujących lub utrudniających użycie jakiegokolwiek złącza wewnętrznego lub zewnętrznego płyty głównej</p> <p>K) obudowa musi posiadać zintegrowany zamek obudowy (nie dopuszcza się klódek lub zabezpieczeń wystających poza obrys obudowy z jakiegokolwiek strony).</p>
JKIW 12	<u>Klawiatura</u> USB w układzie QWERTY (serwisowa).
JKIW 13	<p><u>Mysz:</u></p> <p>A) Panel dotykowy dla użytkowników,</p> <p>B) Mysz optyczna 800 dpi (serwisowa).</p>
JKIW 14	<p><u>Zarządzanie zdalne i diagnostyka:</u></p> <p>Oprogramowanie wyprodukowane i wspierane przez producenta komputera wraz z licencją do zarządzania w sieci, pozwalające minimum na:</p> <p>A) możliwość monitoringu systemu i przekazywania informacji o zdarzeniach na stację administratorską (konsola graficzna na stacji zarządzającej, konsola tekstowa, email lub sms).</p> <p>B) możliwość konfiguracji i weryfikacji zakresu i stopnia szczegółowości alertów przekazywanych na stację administratorską oraz wybór sposobu informacji o zdarzeniu.</p> <p>C) możliwość monitoringu komponentów takich jak: dysk twardy, pamięci, wentylatorów, stanu czujnika otwarcia obudowy, monitoring temperatury wewnętrznej komputera.</p> <p>D) możliwość generowania raportów dot. pojedynczych komputerów lub grup komputerów, w zakresie zainstalowanych komponentów, systemu operacyjnego oraz aplikacji,</p> <p>E) możliwość inwentaryzacji szczegółowej komputera:</p> <ul style="list-style-type: none"> <li>i odczyt modelu, numeru seryjnego i numer inwentarzowego komputera,</li> <li>ii model, wersja firmware i numer seryjny dysku twardego,</li> <li>iii model, wersja firmware i numer seryjny napędu optycznego,</li> </ul> <p>F) oprogramowanie wyprodukowane i wspierane przez producenta komputera pozwalające minimum na:</p> <ul style="list-style-type: none"> <li>i praca w środowisku Windows XP, Windows Vista, Windows 7,</li> <li>ii pełną diagnostykę sprzętową komputera (praca dysku twardego, płyty głównej i jej układów, praca podsystemu pamięci, karty graficznej,</li> </ul>

	<p>iii odczyt informacji o systemie: numer seryjny, numer inwentarzowy,</p> <p>iv eksport informacji do plików danych.</p>
JKIW 15	<p>A) Potwierdzenie kompatybilności komputera na stronie Microsoft Windows Hardware Compatibility List na daną platformę systemową (wydruk ze strony dołączyć do oferty), potwierdzenie producenta o zgodności ze standardami PC 2001, DMI 2.0 (Desktop Management Interface) oraz zWMI 1.5 (Windows Management Instrumentation).</p> <p>B) Deklaracja zgodności CE (dołączyć do oferty).</p> <p>C) Certyfikaty jakości ISO 9001 i 14001 (dołączyć do oferty).</p> <p>D) Certyfikacja Energy Star w wersji co najmniej 5.0 dla oferowanego modelu komputera (do oferty należy dołączyć certyfikat lub zaświadczenie lub wydruk ze strony internetowej).</p> <p>E) Poziom emitowanego hałasu, mierzony wg normy ISO 7779 i wykazany według normy ISO 9296 w trybie jałowym (tryb IDLE ) powinien wynosić nie więcej niż 30 dB z pozycji operatora (potwierdzony stosownym dokumentem producenta komputera). Dopuszcza się dokumenty techniczne w języku angielskim wraz z ich tłumaczeniem.</p>

### 13.7.3 Monitor dotykowy infomatu wewnętrznego

Monitor dotykowy infomatu wewnętrznego musi stanowić zintegrowany układ składający się z wyświetlacza cyfrowego w technologii TN + TFT, zintegrowanego z nakładką dotykową o wymiarach powierzchni aktywnej zgodnych z wymiarami powierzchni użytecznej wyświetlacza.

- W/w układ musi stanowić zwarty moduł, bez luźnych elementów, dostosowany do zabudowy w infomacie i prostej wymiany serwisowej.
- Panel sterowania monitora musi być wyprowadzony na tylną płaszczyznę całego modułu, gdzie jest dostępny od wewnątrz obudowy monitora dotykowego.

#### 13.7.3.1 Wyświetlacz monitora dotykowego infomatu wewnętrznego

Wymagania minimalne dotyczące parametrów wyświetlacza zostały przedstawione w poniższej tabeli:

Wyświetlacz monitora dotykowego infomatu wewnętrznego	
Wymaganie	
WMDIW	Wyświetlacz monitora dotykowego infomatu wewnętrznego musi spełniać niżej wymienione parametry:
WMDIW 1	Rozmiar oraz format: 22" oraz 16:10
WMDIW 2	Rozmiar plamki: 0,282



WMDIW 3	Kąty widzenia: 176° / 176° poziom / pion (CR 5:1)
WMDIW 4	Kontrast:1000:1
WMDIW 5	Jasność : 250 cd/m <sup>2</sup>
WMDIW 6	Czas reakcji matrycy: 5 ms
WMDIW 7	Ilość kolorów:16,7 mln
WMDIW 8	Częstotliwość pozioma: 31,5-82,3 kHz
WMDIW 9	Częstotliwość pionowa: 56 -75 Hz
WMDIW 10	Optymalna rozdzielczość: 1680 x 1050
WMDIW 11	Pozostałe rozdzielczości :1400x1050; 1440x900; 1360x768; 1280x1024; 1280x960; 1280x768; 832x624; 800x600; 720x400; 640x480.
WMDIW 12	Złącze:1x mini D-sub 15 pin; 1x DVI-D
WMDIW 13	Pobór mocy:27w typ; 21W Eco Mode.
WMDIW 14	Certyfikaty: deklaracja CE; ISO 9001 i 14001 dla producenta monitora

### 13.7.3.2 Nakładka dotykowa infomatu wewnętrznego

Wymagania minimalne dotyczące parametrów nakładki dotykowej zostały przedstawione w poniższej tabeli:

Nakładka dotykowa infomatu wewnętrznego	
Parametr	Wartość
NDIW	Nakładka dotykowa infomatu wewnętrznego musi posiadać niżej wymienione parametry:
NDIW 1	Rozmiar: Zgodny z rozmiarem matrycy wyświetlacza.
NDIW 2	Powierzchnia aktywna:450 x 289 mm.
NDIW 3	Technologia wykonania :Technologia pojemnościowa
NDIW 4	Powierzchnia nakładki: Szkło antyodblaskowe o grubości 3,18 mm
NDIW 5	Rozdzielczość minimalna:16K x16K
NDIW 6	Czas reakcji: Poniżej 16 ms
NDIW 7	Przejrzystość:91.5% (±1.5%)
NDIW 8	Twardość powierzchni: 7 punktów w skali Mohsa
NDIW 9	Stabilność: 50 mln dotknięć na punkt bez potrzeby rekalkibracji.
NDIW 10	Siła dotyku: Poniżej 100 g
NDIW 11	Inne: Programowa eliminacja wielopunktowego dotyku

	Wbudowany kontroler USB.
NDIW 12	Certyfikaty: deklaracja CE

### 13.7.4 Obudowa infomatu zewnętrznego

Obudowa infomatu zewnętrznego	
Wymaganie	Minimalne wymagania dotyczące Obudowy infomatu zewnętrznego
OIZ 1	Obudowa infomatu zewnętrznego musi stanowić zwartą bryłę.
OIZ 2	Obudowa infomatu zewnętrznego musi być przeznaczona do montażu naściennego na zewnątrz budynków.
OIZ 3	Korpus obudowy infomatu zewnętrznego wykonany z blachy stalowej o min. grubości 2mm i powierzchni wykończonej fasadową proszkową powłoką lakierniczą, odporną na warunki zewnętrzne.
OIZ 4	Obudowa infomatu zewnętrznego musi być trwale mocowana do ściany za pomocą płyty montażowej.
OIZ 5	Dla celów serwisowych, obudowa infomatu zewnętrznego musi być otwierana od strony frontowej zapewniając dostęp do części wewnętrznych infomatu. Obudowa infomatu musi być wyposażona w zamek z wkładką patentową.
OIZ 6	Obudowa infomatu zewnętrznego musi posiadać konstrukcję uniemożliwiającą dostęp osób niepowołanych do śrub i innych elementów montażowych infomatu oraz jego wyposażenia.
OIZ 7	Obudowa infomatu zewnętrznego musi być wyposażona w system kontroli temperatury pozwalający na pracę infomatu w zakresie temperatur od -20°C do +40°C.
OIZ 8	Obudowa malowana proszkowo farbą poliestrową, drobrnostrukturalną w kolorach wybranych przez Zamawiającego z palety RAL. Przyjmuje się, iż do wszystkich lokalizacji będą dostarczane obudowy w jednym wybranym przez Zamawiającego kolorze.
OIZ 9	Część, w której jest zabudowany monitor, musi zapewniać możliwość korzystania z infomatu przez osoby poruszające się na wózkach inwalidzkich. Przyjmuje się, że elementy do odczytu i wprowadzania danych muszą być w takiej sytuacji dostępne na wysokości 0,9 – 1,1 m od poziomu posadzki, przy czym najwyższy zasięg osoby siedzącej na wózku jest nie wyższy niż 1,4 m.

### 13.7.5 Jednostka komputerowa infomatu zewnętrznego

Jednostka komputerowa infomatu zewnętrznego musi spełniać te same wymagania minimalne, co jednostka komputerowa infomatu wewnętrznego.

### 13.7.6 Monitor dotykowy infomatu zewnętrznego

- Monitor dotykowy infomatu zewnętrznego musi stanowić zintegrowany układ składający się z wyświetlacza cyfrowego w technologii TN + TFT, zintegrowanego z nakładką dotykową o wymiarach powierzchni aktywnej zgodnych z wymiarami powierzchni użytecznej wyświetlacza.
- W/w układ musi stanowić zwarty moduł, bez luźnych elementów, dostosowany do zabudowy w infomacie i prostej wymiany serwisowej.
- Panel sterowania monitora musi być wyprowadzony na tylną płaszczyznę całego modułu, gdzie jest dostępny od wewnątrz infomatu.

#### 13.7.6.1 Wyświetlacz monitora dotykowego infomatu zewnętrznego

Wymagania minimalne dotyczące parametrów wyświetlacza zostały przedstawione w poniższej tabeli:

Monitor dotykowy infomatu zewnętrznego	
Wymaganie	Wartość
MDIZ	Monitor dotykowy infomatu zewnętrznego musi posiadać niżej wymienione parametry:
MDIZ 1	Rozmiar oraz format: 19" oraz 5:4
MDIZ 2	Rozmiar plamki: 0,294
MDIZ 3	Kąty widzenia: 176° / 170° poziom / pion (CR 5:1)
MDIZ 4	Kontrast: 1000:1
MDIZ 5	Jasność: 250 cd/m <sup>2</sup>
MDIZ 6	Czas reakcji matrycy: 5 ms
MDIZ 7	Ilość kolorów: 16,7 mln
MDIZ 8	Częstotliwość pozioma: 30-82 kHz
MDIZ 9	Częstotliwość pionowa: 56 - 75 Hz
MDIZ 10	Optymalna rozdzielczość: 1280 x 1024
MDIZ 11	Pozostałe rozdzielczości: 1280x960; 1152x870; 1152x864; 1024x768; 832x624; 800x600; 720x400; 640x480
MDIZ 12	Złącze: cyfrowe: 1 x DVI-D; analogowe: 1x mini D-sub 15 pin.
MDIZ 13	Pobór mocy: 23W typ; 16W EcoMode

MDIZ 14	Certyfikaty: deklaracja CE ; ISO 9001 i 14001 dla producenta monitora
---------	---

### 13.7.6.2 Nakładka dotykowa infomatu zewnętrznego

Wymagania minimalne dotyczące parametrów nakładki dotykowej zostały przedstawione w poniższej tabeli:

Nakładka dotykowa infomatu zewnętrznego	
Parametr	Wartość
NDIZ 1	Rozmiar: Zgodny z rozmiarem matrycy wyświetlacza.
NDIZ 2	Powierzchnia aktywna: 368mm x 296mm
NDIZ 3	Technologia wykonania: Technologia pojemnościowa
NDIZ 4	Powierzchnia nakładki: Szkło antyodblaskowe o grubości 3,18 mm
NDIZ 5	Rozdzielczość minimalna: 16K x 16K
NDIZ 6	Czas reakcji: Poniżej 16 ms
NDIZ 7	Przejrzystość: 91.5% (±1.5%)
NDIZ 8	Twardość powierzchni: 7 punktów w skali Mohsa
NDIZ 9	Stabilność: 50 mln dotknięć na punkt bez potrzeby rekaliibracji.
NDIZ 10	Siła dotyku: Poniżej 100 g
NDIZ 11	Inne: programowa eliminacja wielopunktowego dotyku; wbudowany kontroler USB.
NDIZ 12	Certyfikaty: deklaracja CE

### 13.7.7 Oprogramowanie infomatu

Oprogramowanie infomatu	
Wymaganie	Minimalne wymagania dotyczące Oprogramowania infomatu
OP I 1	Infomat musi być wyposażony w centralny system zarządzania oraz bezpieczną przeglądarkę internetową posiadającą wyszczególnione poniżej cechy i funkcjonalności.
	<b>Wspólne cechy systemu zarządzania</b>
OP I 2	Brak konieczności instalowania oprogramowania na komputerach administratorów – zarządzanie przez dowolną przeglądarkę internetową.
OP I 3	Zarządzanie odbywać się musi przez stronę www w sposób prosty dla osoby nietechnicznej poprzez aplikacje/serwis www.

OP I 4	Interface użytkownika całkowicie w języku polskim.
OP I 5	Dostęp do serwisu będzie się odbywać przez stronę www z możliwością wykorzystania bezpiecznego protokołu HTTPS z autoryzacją i autentykacją logujących się osób przy pomocy lokalnie przechowywanego certyfikatu elektronicznego.
OP I 6	Strona www do zarządzania będzie działać poprawnie pod przeglądarkami co najmniej trzech różnych producentów (np. Opera, Firefox, Chrome). Strona będzie spełniać standardy XHTML 1.1 transitional oraz przejdzie poprawnie walidację przez zewnętrzny serwis <a href="http://validator.w3.org/">http://validator.w3.org/</a> .
OP I 7	Możliwość pracy pod kontrolą systemów operacyjnych GNU/Linux lub Windows Server.
OP I 8	Komunikacja z infomatami odbywa się jednostronnie. Brak konieczności posiadania zewnętrznych, publicznych adresów IP przez infomaty lub przekierowywania na nie portów.
	<b>Moduł administracji</b>
OP I 9	Musi istnieć możliwość ustawienia parametrów pracy dla aplikacji zainstalowanych w pojedynczym infomacie lub w grupie infomatów wraz z uwzględnieniem hierarchii węzłów.  Realizacja przez system infomatów wirtualnych, z których konfiguracja jest dziedziczona na poszczególne infomaty fizyczne w zależności od przynależności do określonych węzłów struktury, w których znajduje się dany infomat wirtualny.
OP I 10	Dla każdego węzła logicznego musi istnieć możliwość określenia poziomu infrastruktury (np. Centralny, Grupowy, Lokalny, Infomat).
OP I 11	Dla każdego administratora musi istnieć możliwość przydzielenia poziomu infrastruktury (np. Centralny, Grupowy, Lokalny, Infomat).
OP I 12	Dla każdego węzła musi istnieć możliwość przypisania administratora do obsługi danego węzła i ew. wszystkich węzłów podpiętych do niego.
OP I 13	Dla każdego węzła musi istnieć możliwość określenia węzła nadrzędnego.
OP I 14	Musi istnieć możliwość tworzenia dodatkowych kont administratorów.
OP I 15	Dla każdego administratora musi istnieć możliwość podania loginu z hasłem oraz innych dodatkowych informacji np. nr telefonu, adresu e-mail.
	<b>Moduł infomatów</b>

OP I 16	Musi istnieć możliwość przypisania dodatkowych parametrów dla infomatu (np. nazwa, lokalizacja, numer, opis, itp.) ułatwiających ich identyfikację infomatu w systemie. Informacja wyświetlana w formie przyjaznych dymków.
OP I 17	Każdy infomat przynajmniej raz na dobę musi mieć możliwość połączenia się z serwerem centralnym i ściąganie przeznaczone dla niego wygaszacze ekranu, konfigurację, przyciski menu itp.
OP I 18	Każdy infomat przynajmniej raz na dobę musi raportować aplikacji zarządzającej na serwerze centralnym swój bieżący stan działania oraz statystyki aktywności użytkowników.
	<b>Moduł menu</b>
OP I 19	Musi istnieć możliwość definiowania menu jako przyciski na stronie startowej/głównej i w podstawowym oknie przeglądarki.
OP I 20	Musi istnieć możliwość wyboru języka (polski, angielski, niemiecki, rosyjski, ukraiński, słowacki), w którym wyświetlane będą informacje.
OP I 21	Musi istnieć możliwość edycji przycisku (rozmiaru, kolorystyki, czcionki) dla każdej pozycji menu.
OP I 22	Musi istnieć możliwość przypisania gotowej skórki dla każdej pozycji menu.
OP I 23	Musi istnieć możliwość, dla każdej pozycji menu, określenia wyświetlanej na przycisku nazwy powiązanej z dokonaniem wyborem wersji językowej.
OP I 24	Musi istnieć możliwość, dla każdej pozycji menu, określenia adresu URL powiązanego z dokonaniem wyborem wersji językowej.
OP I 25	Musi istnieć możliwość, dla każdej pozycji menu, określenia, czy infomat ma wyświetlić stronę on-line czy off-line.
OP I 26	Musi istnieć możliwość odwołania się z pozycji menu do plików off-line (plik DOC, PDF, HTML).
OP I 27	Musi istnieć możliwość uruchomienia odpowiedniej aplikacji z pozycji menu.
OP I 28	Musi istnieć możliwość, dla każdej pozycji menu, określenia komunikatu, który ma być wyświetlony gdyby link dla niej nie został zdefiniowany lub był nieosiągalny.
OP I 29	Musi istnieć możliwość podglądu zdefiniowanego menu startowego.
	<b>Moduł statystyk i raportów</b>
OP I 30	Każdy infomat przynajmniej raz na dobę musi raportować aplikacji zarządzającej na

	serwerze centralnym swój bieżący stan działania oraz statystyki aktywności użytkowników (logowania, wylogowania, nieuprawnione logowania, restarty, przekroczenia temp. granicznej, alarmy).
OP I 31	Musi istnieć możliwość rejestracji komunikatów o stanie pracy infomatów.
OP I 32	Musi istnieć możliwość grupowania statystyk i podsumowań w ramach zdefiniowanych poziomów infrastruktury.
OP I 33	Musi istnieć możliwość wykonywania zdefiniowanej akcji administracyjnej (komunikat e-mail) w odniesieniu do infomatu, który przez dłuższy niż skonfigurowany czas nie przyśle komunikatu o poprawności pracy.
OP I 34	Musi istnieć możliwość wyświetlenia informacji sprzętowych dotyczących danego infomatu (procesor, dyski twarde, karta graficzna, karta sieciowa, pamięć RAM).
	<b>Moduł wygaszaczy</b>
OP I 35	Musi istnieć możliwość definiowania wygaszaczy ekranu.
OP I 36	Musi istnieć możliwość określania kolejności jak i czasu wyświetlanych wygaszaczy.
OP I 37	Musi istnieć możliwość przypisania źródła wygaszacza (plik, link z zawartością).
OP I 38	Moduł wygaszacza musi obsługiwać następujące typy plików ( JPG, JPEG, PNG, DOC, ODT, PDF, TXT, MP3, WAV, VMA, AVI, MPG, MPEG).
	<b>Moduł zarządzania interfacem przeglądarki</b>
OP I 39	Musi istnieć możliwość zmiany wyglądu poszczególnych elementów aplikacji infomatu na podstawie zdefiniowanych skórek.
OP I 40	Do podstawowych opcji zmiany wyglądu poszczególnych elementów aplikacji zalicza się: A) Zmianę rozmiaru czcionki. B) Zmianę kroju czcionki. C) Zmianę koloru czcionki. D) Zmianę formatowania czcionki (pogrubienie, podkreślenia, pochylenie). E) Zmianę koloru lub obrazka tła.
	<b>Moduł linków</b>
OP I 41	Musi istnieć możliwość filtrowania adresów stron internetowych poprzez moduł edycji linków zabronionych i dozwolonych.

OP I 42	Musi istnieć możliwość bardziej zaawansowanego określania filtrów wykorzystując wyrażenia regularne.
OP I 43	Musi istnieć możliwość przypisywania komunikatów, które pojawią się w momencie wychwycenia linku zabronionego.
	<b>Moduł zadań</b>
OP I 44	Musi istnieć możliwość cyklicznego wywoływania określonych zdarzeń (restart aplikacji, restart systemu, wyłączenia, itp.).
OP I 45	Musi istnieć możliwość dokładnego sprecyzowania czasu wykonania (minuta, godzina, dzień, miesiąc) konkretnego zadania.
	<b>Moduł monitoring</b>
OP I 46	Musi istnieć możliwość sprawdzenia bieżącego stanu infomatu (offline, online).
OP I 47	Musi istnieć możliwość zdalnego wyłączenia i zresetowania infomatu.
OP I 48	Każdy infomat co zadany interwał czasu przysyłać musi do centralnego serwera zarządzającego aktualny zrzut ekranu za pomocą oprogramowania SecureCopy via SSH zabezpieczonego lokalnie przechowywanym certyfikatem elektronicznym.
OP I 49	Musi istnieć możliwość bieżącej obserwacji i analizy danych pobieranych z czujników przy współpracy ze sterownikiem temperatury/wilgotności np. temperatura wewnętrzna, temperatura zewnętrzna. Analiza zmian temperatury stanowić może przydatną informację sugerującą przykładowo konieczność czyszczenia lub wymiany filtrów.
OP I 50	Dane prezentowane muszą być w formie wykresu, który automatycznie odświeża się co zadany interwał czasu. Możliwość przeglądu danych archiwalnych zadanego okresu.
OP I 51	Musi istnieć możliwość określenia wartości granicznych(wyróżnionych również na wykresie), które będą miały wpływ na dalsze działanie infomatu. Przy współpracy ze sterownikiem temperatury/wilgotności musi istnieć możliwość automatycznego wyłączenia monitora i jednostki centralnego po przekroczeniu wartości granicznych (maksymalnej i minimalnej) temperatury wewnątrz infomatu. Po powrocie temperatury do wartości normalnych musi nastąpić automatycznie uruchomienie jednostki centralnej i monitora.
	<b>Moduł zarządzania DigitalSignage</b>
OP I 52	Musi istnieć możliwość konfiguracji:



	<p>A) Biblioteki mediów Playlist (scenariuszy odtwarzania).</p> <p>B) Harmonogramów (dzień, miesiąc, rok).</p> <p>C) Dowolny podział ekranów na strefy.</p> <p>D) Nieograniczona ilość kanałów, playlist, lokalizacji.</p>
OP I 53	<p>Harmonogramowanie wyświetlania playlist umożliwiające:</p> <p>A) Wybranie playlisty, wstawienie jej do harmonogramu oraz wyświetlenie jej w dowolnym czasie i dowolnej strefie.</p> <p>B) Umożliwia ustanowienie harmonogramu na minuta/godzina/dzień/tydzień.</p> <p>C) Z dokładnością do 1 sekundy możliwością ustawienia dowolnego cyklu powtarzania playlisty.</p>
OP I 54	Musi istnieć możliwość powiązania sposobu wyświetlania z określeniem poziomu infrastruktury (aby można było różnicować informacje wg terytorium).
OP I 55	Musi istnieć możliwość gromadzenia statystyk (data, godzina, ilość) emisji materiału.
OP I 56	Wspierane formaty: Video (MPEG1/2/4, AVC, AVI, WMV, DivX), obrazy (JPG, GIF), dźwięk (WMA, MP3), prezentacje / pokaz slajdów, tekst (TXT, plansze tekstowe), kanały RSS (plansze tekstowe, ruchome paski informacyjne), animacje Flash, HTML video (MPEG1/2/4, AVC, AVI, DivX).
	<b>Moduł przeglądarki internetowej</b>
OP I 57	Praca w środowisku Windows oraz GNU/Linux.
OP I 58	Przeglądarka oparta o nowoczesny silnik renderujący Webkit, przechodzący test Acid3w 100% oraz posiadający wsparcie dla technologii HTML5.
OP I 59	Przeglądanie w zakładkach.
OP I 60	Pasek przewijania dostosowany do obsługi poprzez ekran dotykowy.
OP I 61	Musi istnieć możliwość automatycznego powrotu do strony startowej po określonym definiowalnym interwale czasowym.
OP I 62	Musi istnieć możliwość przeglądania stron internetowych zawierających obiekty Flash i Java.
OP I 63	Musi istnieć możliwość Przeglądanie dokumentów PDF, XLS, DOC, ODF.
OP I 64	Musi istnieć możliwość wyboru wyszukiwarki, która będzie ładowana przyciskiem w menu startowym.
OP I 65	Musi istnieć możliwość zablokowania stron z niezaufanym certyfikatem.

OP I 66	Musi istnieć możliwość blokady klawiszy klawiatury Alt, Ctrl, Del, Windows Menu.
OP I 67	Musi istnieć możliwość uruchomienia strony domowej w pełnym oknie.
OP I 68	Musi istnieć możliwość automatycznego włączania (bios) i wyłączenia komputera o określonej godzinie.
OP I 69	Musi istnieć możliwość umieszczenia strony startowej oraz wybranych podstron na dysku lokalnym.
OP I 70	Musi istnieć możliwość kontrolowania systemu okien w celu zablokowania okien określonego typu lub zamknięcia określonych okien, które znalazły się w tle.
OP I 71	Musi istnieć możliwość wyboru i definiowania strony startowej, listy dostępnych funkcji i przycisków w tym przycisku powrotu do strony startowej.
	<b>Moduł e-mail</b>
OP I 72	Moduł musi umożliwiać wysyłanie poczty elektronicznej.
OP I 73	Musi istnieć możliwość włączenia lub wyłączenia modułu.
OP I 74	Musi istnieć możliwość konfiguracji stopki automatycznie dołączanej do każdej wiadomości.
	<b>Moduł bezpieczeństwa</b>
OP I 75	Musi istnieć możliwość zdefiniowania godzin, w jakich informat ma udostępniać Internet.
OP I 76	Musi istnieć możliwość definiowania ustawień, które wpływają na bezpieczeństwo pracy w tym: możliwość blokady ściągania i uruchamiania tzw. cookies, skryptów, apletów Java.
OP I 77	Musi istnieć możliwość definiowania obszarów (zakresów adresów) internetowych, do których użytkownik ma dostęp lub nie. Filtrowanie uwzględniać będzie adresowanie domenowe (DNS) jak i numery IP, oraz umożliwiać dopuszczanie lub blokowanie wskazanych podstron (linków).
OP I 78	Musi istnieć możliwość konfiguracji opcji wygaszania ekranu w połączeniu z dodatkowymi funkcjami takimi jak: automatyczne zamykanie otwartych okien, kasowanie tymczasowych plików, usuwanie historii przeglądarki i rozpoczęcie wyświetlania wskazanej strony.
	<b>Moduł monitoring</b>
OP I 79	Monitorowanie systemu operacyjnego (tzw. Software Watch-Dog), które kontroluje

	zajętość pamięci oraz innych krytycznych elementów systemu i dokonuje jego reinicjalizacji w sytuacji zagrażającej zablokowaniem oprogramowania.
OP I 80	Obsługa Hardware Watch-Dog wykonującego automatyczną reinicjację systemu operacyjnego.
OP I 81	Musi istnieć możliwość przejścia do panelu administracyjnego systemu monitoringu i sterownia temperaturą i wilgotnością (w przypadku zainstalowania takiego modułu w infomacie) wyłącznie za pośrednictwem ekranu dotykowego, po wpisaniu konfigurowalnego hasła z klawiatury ekranowej (brak konieczności otwierania infomatu i podłączania klawiatury).
OP I 82	Musi istnieć możliwość zdalnego podglądu aktualnie wyświetlanego obrazu na infomacie.
OP I 83	Monitorowanie pracy infomatu (m.in. informowanie administratora o pracy infomatu – logowaniu, wylogowaniu, restartach, zabezpieczenie przed nieuprawnioną ingerencją użytkownika w system operacyjny).
	<b>Moduł klawiatury ekranowej</b>
OP I 84	Musi istnieć możliwość przywołania klawiatury w dowolnym momencie.
OP I 85	Musi istnieć możliwość automatycznego wyświetlenia klawiatury ekranowej po wejściu w pola edycyjne.
OP I 86	Musi istnieć możliwość przemieszczania klawiatury po ekranie.
OP I 87	Musi istnieć możliwość konfiguracji stopnia przeźroczystości.
OP I 88	Wyrażna wizualizacja momentu wciśnięcia klawisza poprzez odpowiednią animację.
	<b>Moduł Digital Signage</b>
OP I 89	Musi istnieć możliwość wydzielenia części ekranu infomatu do prezentacji treści multimedialnych.
OP I 90	Musi istnieć możliwość zdefiniowania dowolnej ilości stref w ramach wydzielonego obszaru ekranu.
OP I 91	Musi istnieć możliwość dowolnego przydzielania treści multimedialnych do stref.
OP I 92	Musi istnieć możliwość obsługi następujących formatów: A) obrazki: jpg, bmp, png, B) filmy: avi, mpg, vob, mpeg, C) prezentacji flash: swf,

	<p>D) stron internetowych,</p> <p>E) dokumenty: pdf, ppt, pptx, odp,</p> <p>F) paski informacyjne: tekstowe i rss,</p> <p>G) plansze informacyjne: tekstowe i rss,</p> <p>H) zbieranie danych statystycznych dotyczących wyświetlanie poszczególnych treści.</p>
	<b>Wsparcie dla osób niepełnosprawnych</b>
OP I 93	Musi istnieć możliwość powiększenia treści wyświetlanych w oknie przeglądarki.
OP I 94	Musi istnieć możliwość zmiany pozycji przeglądarki internetowej względem pozostałych treści np. przesunięcie do dolnej krawędzi ekranu w przypadku osoby poruszającej się na wózku inwalidzkim.
OP I 95	Musi istnieć możliwość współpracy z syntezatorem mowy odczytującym treść <u>dowolnej</u> strony internetowej.
	<b>Moduł filtrujący strony internetowe</b>
OP I 96	Musi istnieć możliwość blokady pornografii (także przemocy, hazardu czy rasizmu), nie blokując pojęć encyklopedycznych, haseł związanych z planowaniem rodziny itp.
OP I 97	Filtr musi posiadać bazę adresów zabronionych z możliwości jej automatycznej aktualizacji oraz niezależny moduł oceny stron nie będących w bazie na podstawie ich zawartości.
OP I 98	Filtr przed wyświetleniem strony użytkownikowi musi przypisywać każdemu słowu na stronie punkty. Jeśli słowo jest negatywne (np. "erotyka", "xxx") musi dawać mu plusowe punkty. Jeśli pozytywne (np. "biologia", "rodzina") musi dawać mu punkty ujemne. Na końcu musi sumować całą punktację. Jeśli przekroczy ona limit grzeczności, blokuje ją. Użytkownik zobaczy tylko ostrzeżenie.
	<b>Moduł współpracy z urządzeniami peryferyjnymi</b>
OP I 99	Obsługa czujnika ruchu – dezaktywacja wygaszacza po zbliżeniu użytkownika do infomatu.
OP I 100	Musi istnieć możliwość obsługi czytnika kart bezdotykowych RFID.
OP I 101	Musi istnieć możliwość zarządzania zainstalowanym w infomacie HotSpotem.
	<b>System operacyjny infomatu</b>
OP I 102	Windows Embedded POSReady 7 lub równoważny.

	<p>System równoważny powinien posiadać następujące cechy:</p> <ul style="list-style-type: none"> <li>A) wsparcie dla architektury 32 i 64 bitowej,</li> <li>B) obsługa procesorów wielordzeniowych,</li> <li>C) graficzny okienkowy interfejs użytkownika,</li> <li>D) obsługa co najmniej 8 GB RAM,</li> <li>E) pełna obsługa sprzętu będącego przedmiotem zamówienia (kompatybilność sterowników, w tym sterowników do urządzeń peryferyjnych),</li> <li>F) współpraca z Active Directory, możliwość pracy sieciowej,</li> <li>G) możliwość darmowej aktualizacji poprzez sieć,</li> </ul> <p>posiadający wsparcie pomocy technicznej producenta co najmniej do końca 2015 roku.</p>
	<b>Pozostałe cechy bezpiecznej przeglądarki internetowej</b>
OP I 103	Musi istnieć możliwość automatycznej, nie wymagającej interakcji z użytkownikiem, instalacji oprogramowania („Unattended installation”) za pomocą parametryzacji pliku instalacyjnego.
OP I 104	Przeglądarka musi działać na koncie użytkownika z ograniczonymi prawami natomiast dostęp przeglądarki do sekcji krytycznych systemu operacyjnego musi się odbywać poprzez usługę działającą w kontekście użytkownika bez ograniczeń.
OP I 105	Musi być zapewnione wsparcie dla SSL 128 bit.
OP I 106	Musi istnieć możliwość całkowitej personalizacji interfejsu przeglądarki (możliwość tworzenia własnych skórek - wygląd pasków zadań, przycisków funkcyjnych, klawiatury wirtualnej) bez ingerencji w kod źródłowy przeglądarki.
OP I 107	Musi istnieć możliwość ukrycia paska adresu.
OP I 108	Musi istnieć możliwość aktualizacji i dodawania skórek poprzez system zarządzania.
OP I 109	Musi istnieć możliwość wyświetlania paska postępu ładowania strony WWW.
OP I 110	Musi istnieć możliwość obsługi wirtualnej klawiatury.
OP I 111	Klawiatura wirtualna powinna mieć możliwość wprowadzania polskich znaków diakrytycznych zarówno małych jak i wielkich.
OP I 112	Musi istnieć możliwość minimalizacji lub ukrycia klawiatury, możliwość sterowania/przesuwania klawiaturą.
OP I 113	Musi posiadać wielojęzyczny interfejs, dający możliwość wyboru używanego języka z poziomu konfiguratora przeglądarki.

OP I 114	Musi istnieć możliwość personalizacji wszystkich podpisów przycisków, opisów i komunikatów przeglądarki (dla każdego języka).
OP I 115	Musi istnieć możliwość blokowania uruchamiania javascript, VB script, apletów JAVA, kontrolerek ActiveX.
OP I 116	Musi istnieć możliwość blokowania klawiszy funkcyjnych krytycznych dla systemu operacyjnego (Ctrl+Alt+Del; Shift+F10, Alt+Tab, Alt + Esc, klawisz Windows Log, Ctrl+Esc, Ctrl + Alt + F12).
OP I 117	Musi istnieć możliwość zdefiniowania innych kombinacji klawiszy (przynajmniej trzech), które zostaną zablokowane.
OP I 118	Musi istnieć możliwość zablokowania prawego przycisku myszy.
OP I 119	Musi istnieć możliwość wysyłania wiadomości e-mail z własną stopką definiowalną z poziomu administratora.
OP I 120	Musi istnieć możliwość tworzenia listy stron/domen dozwolonych (pozostałe zabronione) lub zabronionych (pozostałe dozwolone).
OP I 121	Musi istnieć możliwość automatycznego zamykanie niepożądanych okien dialogowych oraz możliwość dopisania nowych typów okien do domyślnie zdefiniowanych.
OP I 122	Musi istnieć możliwość uruchamiania programów zewnętrznych na podstawie stworzonej listy wyboru programów.
OP I 123	Musi istnieć możliwość pracy wielomonitorowej (niezależne wyświetlanie informacji na dwóch monitorach).
OP I 124	Musi istnieć możliwość połączenia z Internetem poprzez LAN, DSL, GPRS lub inną technologię telekomunikacji komórkowej.
OP I 125	Musi istnieć możliwość automatycznego uruchomienia, restartu lub wyłączenia urządzenia o określonej godzinie.
OP I 126	Musi istnieć możliwość zablokowania wyjścia z przeglądarki na definiowalną kombinację klawiszy oraz hasło.
OP I 127	Musi istnieć możliwość zablokowania dostępu do pulpitu - przynajmniej jedno okno przeglądarki pozostaje zawsze otwarte na całym ekranie, bez możliwości zamknięcia lub minimalizacji.
OP I 128	Musi istnieć możliwość automatycznego logowanie do systemu oraz uruchamianie bezpiecznej przeglądarki po uruchomieniu komputera.

OP I 129	Musi istnieć możliwość monitorowania pracy przeglądarki internetowej – w przypadku zawieszenia automatyczny restart aplikacji (możliwość definiowania czasu, po którym następuje restart).
OP I 130	Musi istnieć możliwość uruchamiania wygaszacza ekranu po określonym czasie bezczynności.
OP I 131	Musi istnieć możliwość automatycznego wyczyszczenia historii przeglądanych stron i skasowanie plików tymczasowych oraz Cookie, a następnie powrót do strony startowej po dezaktywacji wygaszacza ekranu lub zakończeniu sesji.
OP I 132	Musi istnieć możliwość zdefiniowania więcej niż jednego wygaszacza ekranu z opcją określenia czasu i kolejności aktywacji.
OP I 133	Musi istnieć możliwość stworzenia listy stron „ulubionych”.
OP I 134	Musi istnieć możliwość blokowania wyskakujących okienek.
OP I 135	Musi istnieć możliwość współpracy z systemem monitoringu i zarządzania.

### 13.7.8 Wdrożenie infomatów

Wdrożenie infomatów	
Wymaganie	Minimalne wymagania dotyczące Wdrożenia infomatów
WINF 1	Wykonawca odpowiada za dostawę, instalację, uruchomienie oraz przetestowanie infomatów. Od Wykonawcy i serwisu infomatów wymagane jest posiadanie certyfikatów ISO 9001, 14001, 27001.
WINF 2	Odbiór wdrożenia infomatu przez Beneficjenta jest równoznaczny z odbiorem dostawy.
WINF 3	Wykonawca przed wdrożeniem musi dostarczyć wzorcowe wersje infomatów, będące przedmiotem zamówienia, celem dokonania stosownych testów oraz weryfikację zgodności z wymaganiami.
WINF 4	Wykonawca musi dostarczyć dokumentację techniczną w postaci rysunków (np. format *.dwg) infomatów wraz z wymiarami oraz wizualizacje graficzne, zdjęcia, karty katalogowe. Rysunki techniczne ukazujące sposób połączenia fundamentów z elementami konstrukcyjnymi obudowy infomatów zewnętrznych i wewnętrznych wolnostojących oraz zewnętrznych i wewnętrznych mocowanych na ścianę.

Zamawiający jest odpowiedzialny za przygotowanie miejsca instalacji infomatu, w tym w szczególności:

- 
- a) Zapewnienie zasilania elektrycznego o właściwych parametrach.
  - b) Zapewnienie łącza logicznego zintegrowanego z infrastrukturą LAN w sposób zapewniający bezpieczeństwo sieci urzędu.
  - c) Przeprowadzenie ewentualnych prac dostosowawczych, w tym również prac remontowo-budowlanych, o ile okażą się konieczne.
  - d) Uzyskanie wszelkich wymaganych prawem pozwoleń.

### **13.8 Dostawa i uruchomienie urządzeń wielofunkcyjnych**

W zakresie dostawy i uruchomienia urządzeń wielofunkcyjnych jest wyposażenie JST w urządzenia zapewniające drukowanie, faksowanie, kopiowanie oraz skanowanie dokumentów w ramach systemu elektronicznego obiegu dokumentów. Jako urządzenie wielofunkcyjne rozumie się jedno urządzenie wykonujące wszystkie przewidziane funkcje.

Wykonawca razem z zestawami urządzeń dostarczy wszelkie niezbędne licencje na wykorzystywane przez urządzenia wielofunkcyjne oprogramowanie wspierające działanie SEOD, w tym licencje dostępowe umożliwiające pracę równoczesną liczbie użytkowników przekraczającej aktualne zapotrzebowanie JST o co najmniej 10%.

#### **13.8.1 Zestaw urządzeń wielofunkcyjnych – wymagania wspólne**

Zestaw urządzeń wielofunkcyjnych zapewniających drukowanie, kopiowanie i skanowanie w wariantach A i B powinny spełniać następujące wymagania:

- Ekran dotykowy na każdym urządzeniu wchodzącym w skład zestawu.
- Funkcja skanowania do E-mail, udziału sieciowego SMB i folderu.
- Funkcja skanowania do PDF, JPEG, TIFF, MTIFF.
- Funkcja wysyłania skanów do wiadomości e-mail bezpośrednio z przedniego panelu urządzenia.
- Funkcja faksowania: faks samoobsługowy lub możliwość podłączenia urządzeń do sieciowego serwera faksu.
- Funkcje drukowania: Automatyczne drukowanie 2-stronne, przechowywanie zleceń (wydruk próbny, zlecenie osobiste (z PIN), szybkie kopiowanie, przechowywanie zleceń (z PIN lub bez PIN)), układ broszury, wiele stron na jednym arkuszu, konfiguracja stron specjalnych (oładki, strony na innym nośniku, strony separujące), znak wodny.
- Bezprzewodowy serwer wydruku.
- Obsługiwane języki opisu strony PCL® 5c / PCL 6.
- Wsparcie systemów operacyjnych: Windows 2000/XP/ Vista/ Server 2003/ Server 2008, 7; AIX, HP-UX, Solaris, Linux, MAC OS.



### 13.8.2 Zestaw urządzeń wielofunkcyjnych – wariant A

Zestaw urządzeń wielofunkcyjnych zapewniających drukowanie, kopiowanie i skanowanie o parametrach nie mniejszych od wartości określonych jako minimalne, wyspecyfikowane w poniższej tabeli.

<b>Zestaw urządzeń wielofunkcyjnych – wariant A</b>	
<b>Wymagania</b>	<b>Urządzenie wielofunkcyjne, kolorowe, A3 o parametrach nie gorszych niż:</b>
ZUW A 1	Technologia druku: kolorowy druk laserowy lub LED, jednoprzebiegowy
ZUW A 2	Gramatura nośników: 60 – 256 g/m <sup>2</sup>
ZUW A 3	Obsługa nośników: Koperta 10, Koperta 7 ¾, A3, A4, A5, Koperta C5, Koperta DL, Executive, Folio, JIS-B4, JIS-B5, Ledger, Legal, Letter, Statement, Universal, Oficio, A6, obsługa nośników nie standardowych 64–297 mm x 148–432 mm
ZUW A 4	Rozdzielczość rzeczywista: 1200dpi x 1200dpi
ZUW A 5	Prędkość druku w kolorze i mono: A3: 22 str./min, A4:40 str./min;
ZUW A 6	Pamięć: 1024 MB
ZUW A 7	Rozbudowa pamięci min do: 2048 MB
ZUW A 8	Wbudowany dysk twardy: 160 GB
ZUW A 9	Procesor: 1,2 GHz
ZUW A 10	Czas wydruku pierwszej strony z trybu gotowości: Poniżej 9,5 sekund
ZUW A 11	Wydajność miesięczna drukowania: 200 000 stron na miesiąc
ZUW A 12	Języki druku/emulacje: PCL, 6, PCL 5c, emulacja PostScript poziom 2 i 3, xHTML, PDF 1.6, Direct Image, Microsoft XPS (XML Paper Specification), AirPrint™
ZUW A 13	Podajniki papieru: A. 1 x 100 arkuszy (obsługa nośników do 256g/m <sup>2</sup> ), B. 1x 520 arkuszy (obsługa nośników do 220 g/m <sup>2</sup> ) C. 1 x 520 arkuszy (obsługa nośników do 220 g/m <sup>2</sup> )
ZUW A 14	Odbiornik papieru: 500 arkuszy
ZUW A 15	Automatyczny duplex: w standardzie wbudowany w urządzenie
ZUW A 16	Panel sterowania: graficzny ekran dotykowy o przekątnej min 10,2 cala;
ZUW A 17	Bezpieczeństwo: możliwość zabezpieczenia drukowanej pracy za pomocą 4 – cyfrowego PIN-u.
ZUW A 18	Porty: 2 x port Hi-Speed USB 2.0, port wbudowanego serwera druku Gigabit Ethernet, port USB 2.0 na panelu urządzenia
ZUW A 19	Opcjonalnie Porty: wewnętrzne serwery druku, zewnętrzne serwery druku,

ZUW A 20	Połączenie sieciowe: wbudowany serwer druku
ZUW A 21	Czcionki: kod kreskowy 3 z 9" w wersji wąskiej, standardowej i szerokiej, 158 skalowalnych czcionek PostScript, 2 czcionki rastrowe PCL, 39 skalowalnych czcionek PPDS, 5 czcionek rastrowych PPDS, 84 skalowalne czcionki PCLOCR-A, OCR-B czcionki skalowalne PCL 5e.
ZUW A 22	Maksymalny obszar zadruku: 297 mm x 1219 mm (banner)
ZUW A 23	Faks: tak; Rozdzielczość faksu standardowo: 200 x 100 dpi. Najwyższa: 600 x 600 dpi, kolor
ZUW A 24	Komunikacja: Możliwość wysyłania poczty e-mail bezpośrednio z urządzenia (z możliwością tworzenie kolorowych załączników *.pdf, *.jpg, *.tiff (mtiff) wpisywanie adresów e-mail , tytułu wiadomości bezpośrednio z panelu urządzenia , współpraca z serwerami LDAP
ZUW A 25	Skanowanie do folderu sieciowego bez potrzeby instalowania dodatkowego oprogramowania
ZUW A 26	Prędkość kopiowania: minimum 44 kopii na minutę
ZUW A 27	Rozdzielczość skanowania/kopiowania: 600x600 dpi
ZUW A 28	Automatyczny podajnik dokumentów – ADF: 100 arkuszy
ZUW A 29	Skanowanie/Kopiowanie dwustronne: wymagane, automatyczne skanowanie/kopiowanie dokumentów dwustronnych
ZUW A 30	Zarządzanie: wbudowany serwer WWW
ZUW A 31	Dostępne opcje: A. Zestaw do tworzenia broszur (ze zszywkami), B. Układarka ze zszywaczem
ZUW A 32	Tonery: Zainstalowane w drukarce; Wydajność: czarny - minimum 19000 stron, kolor - każdy po minimum 12000 stron, (według ISO/IEC 19798).

### 13.8.3 Zestaw urządzeń wielofunkcyjnych – wariant B

Zestaw urządzeń wielofunkcyjnych zapewniających drukowanie, kopiowanie i skanowanie o parametrach związanych z którąś z tych funkcji nie gorszych (tj. nie przekraczających wartości określonych jako maksymalne, ani nie mniejszych od wartości określonych jako minimalne), niż wyspecyfikowane w poniższej tabeli.

Zestaw urządzeń wielofunkcyjnych – wariant B	
Parametry	Urządzenie wielofunkcyjne, kolorowe, A4 o parametrach nie gorszych niż:

ZUW B 1	Technologia druku: kolorowy druk laserowy lub LED, jednoprzebiegowy
ZUW B 2	Gramatura nośników: 60-300 g/m <sup>2</sup>
ZUW B 3	Obsługa nośników: Koperta 10, Koperta 7 ¾, Koperta 9, A4, A5, Koperta B5, Koperta C5, Koperta DL, Executive, Folio, JIS-B5, Legal, Letter, Statement, Universal od 76 x 127 mm do 229 x 356 mm
ZUW B 4	Rozdzielczość rzeczywista: 1200dpi x 1200dpi
ZUW B 5	Prędkość druku w kolorze i mono: 47 str./min A4
ZUW B 6	Pamięć: 1024 MB
ZUW B 7	Rozbudowa pamięci min do: 2048 MB
ZUW B 8	Wbudowany dysk twardy: min 160 GB
ZUW B 9	Procesor: 1,2 GHz
ZUW B 10	Czas wydruku pierwszej strony z trybu gotowości: poniżej 9 sekund
ZUW B 11	Wydajność miesięczna drukowania: 150 000 stron na miesiąc
ZUW B 12	Języki druku/emulacje: Emulacja PCL 5c, Emulacja PCL 6, Personal Printer Data Stream (PPDS), Emulacja PostScript 3, xHTML, PDF 1.6, Direct Image,
ZUW B 13	Podajniki papieru: A. 1 x 100 arkuszy ( obsługa nośników do 220g/m2), B. 1 taca 550 arkuszy
ZUW B 14	Odbiornik papieru: 650 arkuszy
ZUW B 15	Automatyczny duplex: w standardzie, wbudowany w urządzenie
ZUW B 16	Panel sterowania: graficzny ekran dotykowy o przekątnej 10,2 cala; klawisze numeryczne,
ZUW B 17	Bezpieczeństwo: możliwość zabezpieczenia drukowanej pracy za pomocą 4 – cyfrowego PIN-u.
ZUW B 18	Porty: 2 x port Hi-Speed USB 2.0, port wbudowanego serwera druku Gigabit Ethernet, port USB 2.0 na panelu urządzenia
ZUW B 19	Opcjonalnie Porty: wewnętrzne serwery druku, zewnętrzne serwery druku,
ZUW B 20	Połączenie sieciowe: wbudowany serwer druku
ZUW B 21	Czcionki: kod kreskowy"3 z 9" w wersji wąskiej, standardowej i szerokiej, 158 skalowalnych czcionek PostScript, 2 czcionki rastrowe PCL, 39 skalowalnych czcionek PPDS, 5 czcionek rastrowych PPDS, 84 skalowalne czcionki PCL, OCR-A, OCR-B czcionki skalowalne PCL 5e
ZUW B 22	Maksymalny obszar zadruku: 210 x 356 mm
ZUW B 23	Faks: w standardzie
ZUW B 24	Skanowanie: w kolorze

ZUW B 25	Prędkość kopiowania: minimum 42 stron na minutę
ZUW B 26	Rozdzielczość skanowania/kopiowania: 600x600 dpi
ZUW B 27	Automatyczny podajnik dokumentów – ADF: 75 arkuszy
ZUW B 28	Skanowanie/Kopiowanie dwustronne: wymagane, automatyczne skanowanie dokumentów dwustronnych
ZUW B 29	Skanowanie do folderu sieciowego standardowo z poziomu urządzenia
ZUW B 30	Zarządzanie: wbudowany serwer WWW
ZUW B 31	Tonery Pełne, zainstalowane w drukarce; Wydajność: czarny - minimum 12 000 stron, kolor – każdy po minimum 12 000 stron, (według ISO/IEC 19798)

#### 13.8.4 Wdrożenie urządzeń wielofunkcyjnych

Wdrożenie urządzeń wielofunkcyjnych	
Wymaganie	Minimalne wymagania dotyczące Wdrożenia urządzeń wielofunkcyjnych
WUF 1	Wykonawca odpowiada za dostawę, instalację, uruchomienie oraz przetestowanie urządzeń wielofunkcyjnych na przeznaczonych do tego celu stanowiskach komputerowych.
WUF 2	Wykonawca musi zintegrować każdy wdrażany zestaw z wykorzystującym go komputerem stacjonarnym.

#### 13.9 Szafy teleinformatyczne

W ramach projektu Wykonawca zobowiązany będzie o dostarczenie 7 szaf 42 U – dla siedmiu Partnerów. Pozostałe szafy dostarczone zostaną przez wykonawcę wyłonionego przetargu „modernizacja pasywnej infrastruktury sieci urzędów JST”

Szafy teleinformatyczne	
Wymagania	Szafy teleinformatyczne o parametrach nie gorszych niż:
SZT 1	Wysokość szaf 42 U
SZT 2	Rama perforowana z otworami pozwalającymi na łatwy montaż dodatkowego wyposażenia.
SZT 3	Wymagane jest, aby na belkach poziomych otwory były o kształcie kwadratu lub okręgu, ustawione w rozstawie co 25mm, a na belkach pionowych otwory posiadały kształt

	prostokątny lub okrągły w rozstawie co 25mm
SZT 4	Stelaże 19" z możliwością regulacji głębokości w skoku 25mm
SZT 5	Szafy o szerokości 800 mm muszą umożliwiać zamontowanie pionowych listew zasilających o długościach co najmniej 1900 mm w sposób nie ograniczający głębokości użytkowej szafy
SZT 6	Wymiary podstawy: 800 x 1000
SZT 7	Szafy o głębokości 1000 mm i więcej muszą posiadać co najmniej trzy komplety belek wsporczych dla stelaża 19".
SZT 8	Szafy o szerokości 800 mm muszą posiadać zamontowane metalowe wieszaki kablowe pozwalające na prowadzenie wiązki kabli krosowych w pionie bez ograniczenia przestrzeni montażowej 19".
SZT 9	Szafy muszą być pokryte lakierem proszkowym
SZT 10	Szafy muszą być wyposażone w zintegrowany z szafą zestaw co najmniej 6 wentylatorów sufitowych z termostatem, zapewniających wymianę powietrza w szafie oraz efektywne chłodzenie zainstalowanego tam sprzętu aktywnego. Wentylatory nie mogą zajmować miejsca na stelażu 19". Dach szaf powinien posiadać perforację zapewniającą swobodny przepływ powietrza.
SZT 11	Szafy muszą zostać wyposażone w min. 2 panele porządkujące kable krosowe
SZT 12	Szafy muszą posiadać możliwość zainstalowania filtracyjnej zaślepki podłogowej chroniącej przed zasysaniem kurzu do wnętrza szafy.
SZT 13	Szafy muszą posiadać możliwość łączenia w zespoły kilku szaf
SZT 14	Szafy powinny być wyposażone w cokół o wysokości 100 mm.. Cokoły muszą być wyposażone w przeciwwagę, co zapewni stabilność szafy podczas wysuwania zainstalowanego wewnątrz serwera oraz możliwość montażu przepustów szczotkowych z 3 stron
SZT 15	Konstrukcja szafy powinna pozwalać na obciążenie statyczne co najmniej 7000 N z możliwością rozszerzenia poprzez montaż dodatkowych belek nośnych do 10 000 N.
SZT 16	Konstrukcja szafy powinna umożliwiać demontaż na mniejsze elementy umożliwiające zamontowanie w szafy w pomieszczeniu z drzwiami o szerokość 70 cm
SZT 17	Szafy muszą posiadać drzwi przednie perforowane jednoskrzydłowe z czteropunktowym zamknięciem oraz drzwi tylne perforowane dzielone w pionie z zamknięciem trójpunktowym. Drzwi muszą posiadać perforację o prześwicie minimum 80%. Uniwersalna konstrukcja drzwi musi zapewniać możliwość łatwej adaptacji na prawą lub lewą stronę

SZT 18	Szafy muszą posiadać demontowalne osłony boczne oraz osłonę tylną, zapewniające wygodny dostęp do wnętrza szafy z dowolnej strony
SZT 19	Szafy muszą posiadać pełne uziemienie wszystkich sekcji szafy bez konieczności osobnego zamawiania jakichkolwiek elementów uzupełniających. Uziemienie powinno być realizowane za pomocą przewodów miedzianych 6mm <sup>2</sup> . Pojedyncza szyna uziemienia musi posiadać co najmniej 10 punktów mocujących
SZT 20	Szafy muszą zostać podłączone do uziemienia ochronnego (PE) budynkowego za pomocą przewodów miedzianych 10mm <sup>2</sup> prowadzonych w oddzielnych listwach elektroinstalacyjnych. Wszystkie przewody uziemiające powinny być w kolorze żółto – zielonym.
SZT 21	Szafy muszą posiadać w podłodze szczotkowy przepust kablowy o dużej pojemności, a w pozostałej części wypełnienie filtracyjne, minimalizujące przedostawanie się kurzu do wnętrza szafy.
SZT 22	Stopień szczelności IP 20 zgodnie z normą 60529 EN.
SZT 23	Projektant określi w projekcie, a także uzgodni z osobą wyznaczoną w danej JST oraz przedstawicielem Inżyniera Kontraktu, miejsce montażu szaf.

Ponadto dla siedmiu partnerów dla których dostarczane będą opisane powyżej szafy istnieje konieczność dostarczenia kabli przyłączeniowych i krosowych. Ze względu na wymaganą najwyższą trwałość i niezawodność oraz doskonałe parametry kontaktu należy stosować kable przyłączeniowe i krosowe z wtykami RJ45 zarabianymi fabrycznie. Wszystkie kable przyłączeniowe i krosowe muszą być kat. 6, fabrycznie nowe oraz przetestowane przez producenta.

## 14 Promocja projektu

Planowane działania promocyjne i informacyjne będą miały na celu poinformowanie ogółu społeczeństwa o współfinansowaniu projektu ze środków UE w ramach EFRR oraz zwiększenie wiedzy potencjalnych użytkowników PSeAP – u na temat jego możliwości i korzyści, jakie można dzięki systemowi osiągnąć.

Zadania związane z promocją projektu będą realizowane w ramach zadań Wykonawców projektu dostarczających sprzęt dla jednostek samorządu terytorialnego oraz do centrum. Do zadań Wykonawców będzie należało przygotowanie oraz montaż w każdym z miejsc realizacji projektu tablic informacyjnych i pamiątkowych o rozmiarach i treści zgodnej z obowiązującymi wytycznymi. Dodatkowo do zadań Wykonawców projektu będzie należało przygotowanie naklejek na sprzęt i urządzenia, a następnie oznaczanie instalowanych urządzeń w miejscu ich docelowej lokalizacji.

W ramach realizacji umowy Wykonawca zobowiązany będzie do:

### 14.1 Tablice informacyjne i pamiątkowe

Umieszczenia w lokalizacjach w których realizowane będą dostawy tablic informacyjnych oraz pamiątkowych.	
Wymaganie	Minimalne wymagania
TAB 1	Ilość: A) Tablic informacyjnych małych szt. 3 B) Tablic pamiątkowych szt. 160
TAB 2	Zakres prac: Zaprojektowanie (dwa projekty), wykonanie i montaż tablic informacyjnych i pamiątkowych w lokalizacjach realizacji projektu. Projekt podlega akceptacji Zamawiającego.
TAB 3	Wymiary: A) Tablica informacyjna mała format 70 x 90, grubość 3 mm B) Tablica pamiątkowa format 70X90 cm, grubość 3 mm.
TAB 4	Materiał: Tablice pamiątkowe muszą zostać wykonane z trwałego materiału, w technologii odpornej na uszkodzenia mechaniczne i wandalizm (graffiti).
TAB 5	Konstrukcja: do postawienia na metalowym stelażu lub zawieszenia na ścianach wewnątrz

	budynków za pomocą czterech kołków rozporowych.
TAB 6	Montaż: dokładne miejsce montażu wskaże Zamawiający. Adresy lokalizacji w których mają zostać umieszczone tablice informacyjne/pamiątkowe zawiera załącznik nr 2 do OPZ.
TAB 7	Tło: białe
TAB 8	Nadruk: pełny kolor
TAB 9	Obowiązkowa treść tablicy: <ul style="list-style-type: none"> <li>A) logo Narodowej Strategii Spójności w formie znaku programu regionalnego,</li> <li>B) emblemat Unii Europejskiej z napisem „Unia Europejska – Europejski Fundusz Rozwoju Regionalnego”,</li> <li>C) znak promocyjny województwa podkarpackiego z odniesieniem słownym „PODKARPACKIE”,</li> <li>D) informację nt. źródeł finansowania: ”Projekt współfinansowany ze środków Unii Europejskiej z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2007 – 2013”,</li> <li>E) tytuł projektu, nazwa beneficjenta, strona internetowa beneficjenta,</li> <li>F) całkowitą wartość projektu oraz kwota dofinansowania z Europejskiego Funduszu Rozwoju Regionalnego (wartości te powinny być równe wartościom wskazanym w uchwale Zarządu Województwa Podkarpackiego wybierającej projekt do dofinansowania. W przypadku inwestycji, w której po wyborze wykonawcy w przetargu, jej wartość uległa zmianie, IZ RPO WP rekomenduje umieszczenie na tablicy informacyjnej najbardziej aktualnych kwot),</li> <li>G) strona internetowa IZ RPO WP: <a href="http://www.rpo.podkarpackie.pl">www.rpo.podkarpackie.pl</a>,</li> <li>H) hasło określone przez IZ RPO: „Inwestujemy w rozwój województwa podkarpackiego”, podkreślające wartość dodaną pomocy Wspólnoty.</li> </ul>
TAB 10	Tablice pamiątkowe –najpóźniej 14 dni przed zakończeniem terminu realizacji zamówienia.

## 14.2 Plakietki informacyjne

<b>Plakietki informacyjne</b>
-------------------------------



Wymaganie	Minimalne wymagania
PLA 1	Wykonawca zobowiązany jest do oznakowania dostarczanego sprzętu naklejkami informującymi o dofinansowaniu Projektu ze środków UE.
PLA 2	Ilość sztuk: równa ilości dostarczonego sprzętu wyspecyfikowanego w załączniku nr 1 do niniejszego OPZ. W przypadku zestawów komputerowych naklejką powinny być oznaczony komputer, monitor oraz klawiatura.
PLA 3	Tło: Białe
PLA 4	Nadruk: Pełny kolor
PLA 5	<p>Plakietka informacyjna stosowana podczas realizacji projektu musi zawierać minimum:</p> <ul style="list-style-type: none"> <li>A) logo Narodowej Strategii Spójności w formie znaku programu regionalnego,</li> <li>B) emblemat Unii Europejskiej z napisem „Unia Europejska – Europejski Fundusz Rozwoju Regionalnego”,</li> <li>C) znak promocyjny województwa z odniesieniem słownym „PODKARPACKIE”,</li> <li>D) informację nt. źródeł finansowania: „Zakup współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2007 – 2013”,</li> <li>E) hasło określone przez IZ RPO: „Inwestujemy w rozwój województwa podkarpackiego”, podkreślające wartość dodaną pomocy Wspólnoty Europejskiej.</li> </ul>
PLA 6	<p>Wymiary:</p> <ul style="list-style-type: none"> <li>A) Minimalny rozmiar plakietki powinien mieć wymiary 10 cm (szerokość) x 6,5 cm (wysokość). Jeżeli niemożliwe lub niezasadne byłoby umieszczenie plakietki o takich rozmiarach, dopuszcza się zmniejszenie rozmiaru do takiej wielkości, aby plakietka nadal była czytelna.</li> <li>B) W przypadku przedmiotów na których nie ma możliwości zamieszczenia czytelnej informacji o dofinansowaniu, możliwe jest zamieszczenie informacji na opakowaniu/etui sprzętu, przy czym musi to być opakowanie/etui użytkowane łącznie ze sprzętem (nie może być to opakowanie kartonowe, w którym sprzęt został zakupiony).</li> </ul>

---

### 14.3 Wymaganie ogólne

Projekty materiałów informacyjno-promocyjnych muszą zostać zaakceptowane przez Zamawiającego. Przez pojęcie „projekt” należy rozumieć opracowanie graficzne i merytoryczne (treści) materiałów promocyjnych.

Wszystkie przygotowywane dokumenty muszą zostać oznaczone zgodnie z wymaganiami zawartymi w wytycznych Instytucji Zarządzającej RPO WP na lata 2007- 2013 dla beneficjentów w zakresie informacji i promocji.

## 15 Gwarancje

Gwarancje	
Wymaganie	Minimalne wymagania dotyczące Serwisu gwarancyjnego i wsparcia eksploatacyjnego dla systemu SEOD i SeUI
	<b>Ogólne</b>
GWA 1	Wykonawca zobowiązany jest do świadczenia serwisu gwarancyjnego przez okres minimum <b>36</b> miesięcy od dnia odbioru wdrożenia Systemu przez Zamawiającego.
GWA 2	Wykonawca zobowiązany jest do świadczenia wsparcia eksploatacyjnego od dnia odbioru wdrożenia Systemu przez Zamawiającego, do dnia zakończenia Fazy Eksploatacyjnej Projektu.
GWA 3	Dla potrzeb związanych z realizacją usług serwisu gwarancyjnego i wsparcia eksploatacyjnego, Zamawiający zapewni Wykonawcy zdalny dostęp do swoich instalacji Systemu.
GWA 4	Zamawiający wymaga, aby zgłoszenia problemów technicznych były dokonywane drogą elektroniczną przez osoby odpowiedzialne i upoważnione po stronie Zamawiającego, mającą dostęp do portalu poprzez login i hasło. (Do oferty należy dołączyć link do portalu serwisowego, login oraz hasło do testowego użytkownika systemu).
	<b>Wymagania zakresu usług serwisu gwarancyjnego i wsparcia eksploatacyjnego SEOD i SeUI</b>
	<b>Ogólne</b>
GWA 5	Serwis gwarancyjny systemów musi obejmować co najmniej: <ul style="list-style-type: none"> <li>A) Prowadzenie przez Wykonawcę systemu pomocy zdalnej – „Help Desk”, dostępnego dla wszystkich użytkowników Systemu.</li> <li>B) Help Desk musi świadczyć co najmniej następujące rodzaje pomocy zdalnej: <ul style="list-style-type: none"> <li>i Przyjmowanie zgłoszeń dotyczących błędnego działania Systemu, w tym telefonicznie, faksem i mailem. Zgłaszanie problemów tymi drogami powinno być możliwe telefonicznie i faksem między 8:30 a 16:30.</li> <li>ii Bieżące informowanie zgłaszających błędy użytkowników o diagnozie</li> </ul> </li> </ul>

	<p>przyczyn zgłoszonego błędu, przewidywanym terminie usunięcia błędu, statusie zainicjowanej zgłoszeniem błędu procedury obsługi zgłoszenia.</p> <p>iii Udzielanie wskazówek oraz wyjaśnień dotyczących zasad efektywnej pracy z Systemem w zakresie obejmującym przynajmniej zawartość dostarczonych przez Wykonawcę szkoleń dla zwykłych użytkowników Systemu.</p> <p>C) Help Desk musi rejestrować wszelkie kontakty z użytkownikami Systemu jako nowe zgłoszenia, lub jako elementy przyporządkowane do toczących się procedur obsługi istniejących zgłoszeń.</p> <p>D) Help Desk musi posiadać stronę webową, za pomocą której każdy użytkownik Systemu może sprawdzić status zainicjowanych przez siebie procedur obsługi zgłoszeń. Ponadto zgłoszenia i ich statusy muszą być publikowane automatycznie w Portalu CPI.</p>
GWA 6	<p>Klasyfikowanie, diagnozowanie oraz rozwiązywanie błędów zgłaszanych przez użytkowników Systemu.</p> <p>A) Fakt wystąpienia błędu, oraz jego ewentualną charakterystykę, ocenia się zawsze w odniesieniu do ostatniej wersji opisu funkcjonalnego Systemu, uzgodnionej pomiędzy Zamawiającym a Wykonawcą.</p> <p>B) Przez rozwiązanie błędu, lub ostateczne rozwiązanie błędu, rozumie się wdrożenie działań, dzięki którym dany błąd przestaje występować podczas zgodnego z przeznaczeniem korzystania z funkcji Systemu.</p> <p>C) Przez obejście błędu rozumie się przekazanie do wiadomości Beneficjenta szczegółowego opisu działań, dzięki którym procedury użycia Systemu, będące normalnie pod wpływem danego błędu, mogą zostać przeprowadzone w sposób wykluczający powstanie i / lub wpływ tego błędu.</p> <p>D) Błędy muszą być klasyfikowane według stopnia ich wpływu na dostępność funkcji Systemu, jako:</p> <p>i Błędy krytyczne, tzn. takie błędy, w wyniku których co najmniej jedna komórka organizacyjna urzędu w ogóle nie może realizować swojej funkcji statutowej przy pomocy Systemu, lub żadna z funkcji statutowych urzędu nie może być w pełni zrealizowana przy pomocy Systemu na skutek ujawnienia się wady tego Systemu.</p> <p>ii Błędy poważne, tzn. takie błędy, w wyniku których co najmniej jedna komórka organizacyjna urzędu napotyka w Systemie na ograniczenia ilościowe lub funkcjonalne uniemożliwiające realizację pełnego zakresu jej funkcji statutowej przewidzianego do realizacji przy</p>

	<p>pomocy Systemu na skutek ujawnienia się wady tego Systemu.</p> <p>iii Pozostałe błędy, tzn. takie błędy, w wyniku których przeprowadzenie określonych operacji w Systemie jest niemożliwe, lub daje niepoprawny rezultat na skutek ujawnienia się wady tego Systemu.</p> <p>E) Maksymalne wartości parametrów czasowych opisujących reakcję serwisową Wykonawcy w przypadku wystąpienia poszczególnych kategorii błędów Systemu mogą wynosić co najwyżej (przez godziny rozumie się poniżej godziny zegarowe niezależnie od tego, czy są to godziny lub dni robocze, czy nie):</p> <p>i Dla błędów krytycznych – reakcja w ciągu 1 godziny, przywrócenie funkcjonowania systemu (rozwiązanie lub obejście błędu) w ciągu 12 godzin od przyjęcia zgłoszenia błędu, ostateczne rozwiązanie problemu w ciągu 96 godzin od zgłoszenia błędu.</p> <p>ii Dla błędów poważnych – reakcja w ciągu 2 godzin, przywrócenie pełnej funkcjonalności systemu (rozwiązanie lub obejście błędu) w ciągu 20 godzin od przyjęcia zgłoszenia błędu, ostateczne rozwiązanie problemu w ciągu 240 godzin od zgłoszenia błędu.</p> <p>iii Dla pozostałych błędów – reakcja w ciągu 48 godzin od przyjęcia zgłoszenia błędu, rozwiązanie ostateczne w najbliższej nowej wersji oprogramowania Systemu, nie później niż w ciągu 3 miesięcy od zgłoszenia błędu.</p> <p>F) Przez reakcję rozumie się kontakt ze strony przedstawiciela wykonawcy, potwierdzenie zgłoszenia oraz rozpoczęcie działań diagnostycznych.</p> <p>G) Dla błędów w systemie SEOD, jeśli termin przywrócenia funkcjonowania systemu lub termin ostatecznego rozwiązania błędu przypada w dzień ustawowo wolny od pracy, w sobotę lub między godz. 18:00 a 7:00 rano, wówczas ulega on przesunięciu na godz. 7:00 najbliższego dnia roboczego.</p> <p>H) Ostateczne rozwiązanie błędu wymagającego poprawy kodu oprogramowania Systemu musi obejmować wytworzenie oraz przekazanie do dyspozycji Beneficjenta stosownej aktualizacji oprogramowania Systemu.</p> <p>i Każda aktualizacja oprogramowania może zawierać poprawki kodu oprogramowania dotyczące jednego lub więcej zgłoszonych błędów.</p> <p>ii Wszystkie znajdujące się w aktualizacji oprogramowania poprawki kodu oprogramowania muszą być udokumentowane w sposób umożliwiający przynajmniej ustalenie istoty błędu usuwanego przez daną poprawkę.</p>
GWA 7	<u>Dostawę nowych wersji oprogramowania Systemu.</u>

	<p>A) Wykonawca może przekazać Zamawiającemu nową wersję oprogramowania Systemu dopiero po wszechstronnej weryfikacji poprawności jej działania w środowisku testowym, odzwierciedlającym typowe środowisko produkcyjne spotykane u Beneficjentów.</p> <p>B) Razem z nową wersją oprogramowania, Wykonawca musi dostarczyć zaktualizowaną dokumentację Systemu.</p> <p>C) Po wdrożeniu nowej wersji oprogramowania w Systemie Beneficjenta, Wykonawca ponosi odpowiedzialność na tych samych zasadach za działanie odnośnego SEOD, jaką ponosił w stosunku do uprzednio tam działającej wersji Systemu.</p> <p>D) Wersja zdeponowana kodów źródłowych musi być każdorazowo aktualizowana w przypadku zmian lub aktualizacji wersji produkcyjnej.</p>
GWA 8	<p><u>Utrzymywanie Systemu w zgodności ze stanem prawnym.</u></p> <p>Wszelkie wynikające ze zmian stanu prawnego modyfikacje parametrów konfiguracyjnych lub danych wprowadzonych do Systemu leżą po stronie Beneficjenta. Wszelkie zmiany funkcjonalne systemu SeUI wynikające z wymagań prawnych są po stronie beneficjenta. Wszelkie zmiany funkcjonalne systemu SEOD wynikające z wymagań prawnych w okresie gwarancji są po stronie Wykonawcy.</p>
	<p><b><u>Wsparcie eksploatacyjne SEOD</u></b></p>
GWA 9	<p><u>Wsparcie eksploatacyjne SEOD musi obejmować co najmniej:</u></p> <p>A) Wsparcie zarządzania konfiguracją serwerów aplikacyjnych SEOD, w tym:</p> <ul style="list-style-type: none"> <li>i Wsparcie administrowania oprogramowaniem systemowym oraz bazodanowym serwera poprzez okresowe, co najmniej raz na rok konsultacje ustawień konfiguracyjnych.</li> <li>ii Instalację niezbędnych aktualizacji oprogramowania SEOD niezbędnych do pracy zgodnej z dokumentacją.</li> <li>iii Modyfikację parametrów konfiguracyjnych lub danych oprogramowania SEOD, o ile nie leży to po stronie Beneficjentów z tytułu dostosowania Systemu do zmiany stanu prawnego.</li> </ul> <p>B) Wdrażanie nowych wersji oprogramowania SEOD, w tym:</p> <ul style="list-style-type: none"> <li>i Instalację nowych wersji oprogramowania aplikacyjnego SEOD na serwerach Beneficjentów.</li> <li>ii Modyfikację parametrów konfiguracyjnych lub danych wprowadzonych do oprogramowania SEOD, o ile nie leży to po stronie Beneficjentów z tytułu dostosowania Systemu do zmiany stanu prawnego.</li> <li>iii Uruchamianie nowych wersji oprogramowania aplikacyjnego SEOD.</li> </ul>

	<b>Wsparcie eksploatacyjne SeUI</b>
GWA 10	<p><u>Zarządzanie konfiguracją platformy serwera SeUI, w tym:</u></p> <ul style="list-style-type: none"> <li>A) Wsparcie administrowania oprogramowaniem systemowym oraz bazodanowym serwera poprzez okresowe, co najmniej raz na rok konsultacje ustawień konfiguracyjnych.</li> <li>B) Instalację niezbędnych aktualizacji oprogramowania aplikacyjnego SeUI.</li> <li>C) Wdrażanie i likwidowanie obejść błędów.</li> <li>D) Modyfikację parametrów konfiguracyjnych lub danych oprogramowania SeUI, o ile nie leży to po stronie Zamawiającego z tytułu dostosowania Systemu do zmiany stanu prawnego.</li> </ul>
GWA 11	<p><u>Wdrażanie nowych wersji oprogramowania SeUI, w tym:</u></p> <ul style="list-style-type: none"> <li>A) Instalację nowych wersji oprogramowania aplikacyjnego SeUI.</li> <li>B) Modyfikację parametrów konfiguracyjnych lub danych wprowadzonych do oprogramowania SeUI, o ile nie leży to po stronie Zamawiającego z tytułu dostosowania Systemu do zmiany stanu prawnego.</li> <li>C) Uruchamianie nowych wersji oprogramowania aplikacyjnego SeUI.</li> </ul>
GWA 12	W przypadku konieczności zmiany dokumentacji w wyniku dokonania naprawy Wykonawca zobowiązany jest doręczyć zaktualizowaną dokumentację maksymalnie w 14 dni po zakończeniu naprawy.
	<b>Minimalne wymagania dotyczące Serwisu gwarancyjnego i wsparcia eksploatacyjnego Sprzętu</b>
GWA 13	Co najmniej 36 miesięczna gwarancja.
GWA 14	Czas reakcji serwisu - do końca następnego dnia roboczego.
GWA 15	<ul style="list-style-type: none"> <li>A) Serwis musi być realizowany zgodnie z wymaganiami normy ISO 9001 – do oferty należy dołączyć dokument potwierdzający, że serwis będzie realizowany zgodnie z tą normą. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta.</li> </ul>
GWA 16	W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.
GWA 17	Reakcja serwisowa dla komputerów biurowych i przenośnych będzie zawsze

	realizowana w miejscu instalacji sprzętu.																														
GWA 18	Beneficjent odpowiada za fizyczne udostępnienie sprzętu w celu umożliwienia realizacji reakcji serwisowej przez personel Wykonawcy.																														
GWA 19	Czas oczekiwania na fizyczne udostępnienie sprzętu nie jest uwzględniany w statystykach jakościowych świadczonego serwisu.																														
GWA 20	Reakcja serwisowa obejmuje diagnozę przyczyn awarii, wymianę komponentów sprzętu w zakresie niezbędnym do usunięcia awarii oraz weryfikację stopnia powodzenia podjętych działań.																														
GWA 21	Pod względem charakterystyki wydajnościowej i funkcjonalnej, nowe komponenty sprzętowe nie mogą ustępować komponentom, w miejsce których zostały dostarczone lub zainstalowane.																														
GWA 22	Wykonawca zatrzymuje odebrane lub wymontowane komponenty sprzętu.																														
GWA 23	<p>Poniższa tabela zawiera zestawienie wymaganych parametrów serwisu gwarancyjnego dla poszczególnych kategorii sprzętu. Określenia „dzień (roboczy)” oraz „godzina” odnoszą się do dni / godzin pracy Beneficjenta.</p> <table><tr><th>Kategoria Sprzętu</th><th>Maksymalny czas rejestracji zgłoszenia</th><th>Maksymalny czas usunięcia awarii</th></tr><tr><td>Zestaw serwerowy oraz pozostałe wyposażenie w CPD</td><td>2 godziny (w dni robocze)</td><td>8 godzin (w dni robocze)</td></tr><tr><td>Zestaw serwerowy u Partnera</td><td>4 godziny (w dni robocze)</td><td>2 dni robocze</td></tr><tr><td>Urządzenia sieciowe</td><td>4 godziny (w dni robocze)</td><td>2 dni robocze</td></tr><tr><td>Podpis elektroniczny</td><td>1 dzień roboczy</td><td>5 dni roboczych</td></tr><tr><td>Komputer biurowy</td><td>2 dni robocze</td><td>8 dni roboczych</td></tr><tr><td>Komputer przenośny typu „notebook”.</td><td>2 dni robocze</td><td>8 dni roboczych</td></tr><tr><td>Urządzenia wielofunkcyjne</td><td>1 dzień roboczy</td><td>5 dni roboczych</td></tr><tr><td>Mysz i klawiatura.</td><td>2 dni robocze</td><td>5 dni roboczych</td></tr><tr><td>Monitor.</td><td>2 dni robocze</td><td>5 dni roboczych</td></tr></table>	Kategoria Sprzętu	Maksymalny czas rejestracji zgłoszenia	Maksymalny czas usunięcia awarii	Zestaw serwerowy oraz pozostałe wyposażenie w CPD	2 godziny (w dni robocze)	8 godzin (w dni robocze)	Zestaw serwerowy u Partnera	4 godziny (w dni robocze)	2 dni robocze	Urządzenia sieciowe	4 godziny (w dni robocze)	2 dni robocze	Podpis elektroniczny	1 dzień roboczy	5 dni roboczych	Komputer biurowy	2 dni robocze	8 dni roboczych	Komputer przenośny typu „notebook”.	2 dni robocze	8 dni roboczych	Urządzenia wielofunkcyjne	1 dzień roboczy	5 dni roboczych	Mysz i klawiatura.	2 dni robocze	5 dni roboczych	Monitor.	2 dni robocze	5 dni roboczych
Kategoria Sprzętu	Maksymalny czas rejestracji zgłoszenia	Maksymalny czas usunięcia awarii																													
Zestaw serwerowy oraz pozostałe wyposażenie w CPD	2 godziny (w dni robocze)	8 godzin (w dni robocze)																													
Zestaw serwerowy u Partnera	4 godziny (w dni robocze)	2 dni robocze																													
Urządzenia sieciowe	4 godziny (w dni robocze)	2 dni robocze																													
Podpis elektroniczny	1 dzień roboczy	5 dni roboczych																													
Komputer biurowy	2 dni robocze	8 dni roboczych																													
Komputer przenośny typu „notebook”.	2 dni robocze	8 dni roboczych																													
Urządzenia wielofunkcyjne	1 dzień roboczy	5 dni roboczych																													
Mysz i klawiatura.	2 dni robocze	5 dni roboczych																													
Monitor.	2 dni robocze	5 dni roboczych																													



GWA 24	W czasie trwania okresu gwarancji, Wykonawca zobowiązany jest do zapewnienia Beneficjentom dostępu do nowych wersji BIOS, firmware i sterowników dla sprzętu objętego gwarancją (na płytach CD lub stronach internetowych).		
	<b>Minimalne wymagania dotyczące Serwisu gwarancyjnego Infomatów</b>		
GWA 25	Usterki mogą być zgłaszane za pośrednictwem infolinii - ogólnopolskiego numeru o zredukowanej odpłatności 0-800/0-801, dedykowanego do obsługi zgłoszeń serwisowych. Zamawiający wymaga, aby Wykonawca uruchomił lub udostępnił numer infolinii w dniu dokonania odbioru infomatów.		
GWA 26	Uzyskanie danych o dostarczonych produktach w szczególności o terminie ważności gwarancji.		
GWA 27	Uzyskanie informacji o elementach składowych produktu, jeżeli jest wytworzony przez Wykonawcę.		
GWA 28	Podgląd dokonanych w trakcie eksploatacji wymian podzespołów.		
GWA 29	Podgląd dołączonych do produktu dokumentów, w szczególności certyfikatów, zaświadczeń.		
GWA 30	Uzyskanie historii awarii produktu oraz podjętych interwencji.		
GWA 31	Powiadamianie Zamawiającego drogą elektroniczną (np. e-mail) o podjętych czynnościach w ramach zarejestrowanego zgłoszenia (np. określenie terminu usunięcia usterki, określenie terminu planowanej wizyty serwisowej wraz z opisem planowanych czynności, zamknięcie zgłoszenia serwisowego).		
GWA 32	Możliwość zgłaszania propozycji dotyczących funkcjonalności oprogramowania.		
GWA 33	Możliwość zgłaszania błędów w oprogramowaniu.		
GWA 34	Zarejestrowanie zgłoszenia reklamacyjnego.		
GWA 35	Śledzenie stanu obsługi zgłoszenia reklamacyjnego od momentu zarejestrowania do jego zamknięcia.		
GWA 36	Wymagane parametry serwisu gwarancyjnego dla poszczególnych kategorii sprzętu		
	Wymaganie	Kategoria Sprzętu	Maksymalny czas serwisowej rejestracji zgłoszenia
	SG KS 1	Obudowa	2 dni robocze
	SG KS 2	Jednostka komputerowa	3 dni robocze
			Maksymalny czas usunięcia awarii
			4 tygodnie
			5 dni roboczych

	SG KS 3	Monitor dotykowy	Następny dzień roboczy	2 dni robocze
	<b>Minimalne wymagania dotyczące serwisu gwarancyjnego urządzeń wielofunkcyjnych</b>			
GWA 37	Gwarancja na dostarczone zestawy do przyjmowania dokumentów musi obowiązywać przez co najmniej 60 miesięcy od daty odbioru sprzętu.			
GWA 38	Gwarancja nie obejmuje materiałów i części eksploatacyjnych zgodnie z gwarancją producenta, które użytkownik musi uzupełniać we własnym zakresie.			
GWA 39	Wykonawca zapewni punkt przyjmowania zgłoszeń serwisowych dotyczących sprzętu objętego gwarancją, dostępny drogą telefoniczną w dni pracy użytkowników w godzinach 8:30 - 16:30			
GWA 40	Reakcja serwisowa jest zawsze realizowana w miejscu instalacji sprzętu. Użytkownik odpowiada za fizyczne udostępnienie sprzętu w celu umożliwienia realizacji reakcji serwisowej przez personel Wykonawcy. Czas oczekiwania na fizyczne udostępnienie sprzętu nie jest uwzględniany w statystykach jakościowych świadczonego serwisu.			
GWA 41	Reakcja serwisowa obejmuje diagnozę przyczyn awarii. Pod względem charakterystyki wydajnościowej i funkcjonalnej, nowe komponenty sprzętowe nie mogą ustępować komponentom, w miejsce których zostały dostarczone lub zainstalowane. Wykonawca zatrzymuje wszystkie odebrane lub wymontowane komponenty sprzętu.			
GWA 42	W czasie trwania okresu gwarancji, Wykonawca zobowiązany jest do zapewnienia użytkownikom dostępu do nowych wersji sterowników dla sprzętu objętego gwarancją (na płytach CD lub stronach internetowych).			
GWA 43	Maksymalny czas podjęcia reakcji serwisowej to następny dzień roboczy licząc od dnia zgłoszenia awarii.			
	<b>Minimalne wymagania dotyczące Serwisu gwarancyjnego i wsparcia eksploatacyjnego Oprogramowanie</b>			
GWA 44	W cenie oferowanego wsparcia zawarte muszą być również uaktualnienia oferowanego oprogramowania (oprogramowania, licencji) do najnowszej wersji uwzględniające współpracę z ukazującymi się na rynku nowymi rozwiązaniami sprzętowymi i programowymi.			
	<b>Minimalne wymagania dotyczące Serwisu gwarancyjnego na szafy serwerowe/teleinformatyczne</b>			

---

GWA 45	5 letni okres gwarancji
--------	-------------------------

## 16 Licencje

Wymaganie	Minimalne wymagania dotyczące licencji
	<b>Ogólne</b>
LIC 1	Wykonawca obowiązany jest dostarczyć wszystkie licencje oprogramowania niezbędne do prawidłowego funkcjonowania Systemu PSeAP w zakładanym kształcie. Wykonawca dostarczy komplet licencji na potrzeby systemów SeUI oraz SEOD, w tym licencje oprogramowania pomocniczego i oprogramowania podstawowego. Te licencje powinny umożliwiać pracę przy założeniu, że liczba użytkowników korzystających z systemu będzie wynosić do 110% liczby użytkowników podanej dla każdego Partnera w Załączniku 1.
LIC 2	Wszystkie licencje będą udzielone bezterminowo, nie będą także w żaden sposób ograniczać pojemności Systemu PSeAP ani liczby dokonywanych w Systemie operacji.
LIC 3	Wykonawca przekaże Zamawiającemu niewyłączne prawa autorskie do oprogramowania autorskiego wykorzystanego w systemie PSeAP. Prawa te będą umożliwiały Zamawiającemu i Partnerom Projektu rozwój i modyfikację ww. oprogramowania na własne potrzeby, potrzeby Partnerów Projektu oraz innych jednostek samorządu terytorialnego województwa podkarpackiego, a także ich jednostek podległych, wyłącznie w przypadku, gdy: <ul style="list-style-type: none"> <li>A) zajdzie konieczność dostosowania oprogramowania do zmian prawnych i dostosowanie to nie będzie przedmiotem bezpłatnej aktualizacji udostępnionej przez Wykonawcę lub Wykonawca nie daje rękojmi dostosowania oprogramowania do zmian prawnych do dnia ich wejścia w życie;</li> <li>B) Wykonawca upadnie lub zaprzestanie działalności lub zaprzestanie lub zawiesi rozwijanie oprogramowania autorskiego.</li> </ul>
LIC 4	Aby umożliwić Zamawiającemu korzystanie w dowolnym czasie z prawa autorskiego na warunkach określonych powyżej, Wykonawca zdeponuje kody źródłowe autorskiego oprogramowania, wszystkie niezbędne biblioteki i moduły umożliwiające prawidłową kompilację SEOD oraz dokumentację techniczną oprogramowania (co najmniej specyfikacje interfejsów komponentów wraz z określeniem poszczególnych funkcji, model obiektowy, model bazy danych wraz z opisem znaczenia poszczególnych wartości, dokumentację poszczególnych klas wygenerowaną automatycznie, instrukcję kompilacji) w takim zakresie, by po okresie gwarancji możliwe było samodzielne utrzymanie systemu PSeAP,



	<p>w szczególności SEOD, przez Partnerów, w tym dokonanie aktualizacji bezpieczeństwa oraz dostosowanie do zmian prawnych. Kody źródłowe i szczegółowa procedura dot. przebiegu czynności kompilacji winny być zdeponowane w wersji elektronicznej, redundantnie - na dwóch nośnikach o gwarantowanej trwałości (nie krótszej niż 10 lat) w zalakowanych kopertach. Na tych samych warunkach Wykonawca zdeponuje kody źródłowe w przypadku dokonywania modyfikacji lub aktualizacji oprogramowania.</p>
LIC 5	<p>Dobór oprogramowania licencyjnego na potrzeby realizacji PSeAP oraz warunki udzielonych licencji na to oprogramowanie nie mogą ograniczać możliwości utrzymania i rozwoju Systemu PSeAP przez Zamawiającego i Partnerów Projektu w zakresie funkcjonalności dedykowanych dla administracji publicznej i wynikających z przepisów prawa oraz w zakresie funkcjonalności dedykowanych dla Projektu PSeAP. Oznacza to w szczególności, że jeśli SEOD lub dedykowane komponenty SeUI są rozwiązaniami autorskimi podmiotów trzecich, prawa do modyfikacji i rozwoju muszą także zostać udzielone Zamawiającemu i Partnerom a kody źródłowe zdeponowane pod takimi samymi warunkami, jak wskazano dla oprogramowania autorskiego w wymaganiu LIC 3, co najmniej w zakresie zabezpieczającym możliwość utrzymania systemu i dostosowania do zmian prawnych np. w przypadku upadłości czy zaprzestania działalności producenta oprogramowania.</p>
LIC 6	<p>Udzielone licencje będą uprawniały Partnerów Projektu do modyfikacji wszystkich konfigurowalnych parametrów oprogramowania, reinstalacji oprogramowania z posiadanych nośników.</p>
LIC 7	<p>A) W zakresie wszystkich elementów oprogramowania licencyjnego Zamawiający wymaga dostarczenia kompletu wymaganych kluczy aktywacyjnych, jeśli są potrzebne do uruchomienia danego elementu oprogramowania.</p> <p>B) Zamawiający wymaga, aby wszystkie te licencje zostały wystawione przez producenta imiennie dla każdego partnera( JST) uczestniczącego w postępowaniu, który będzie z nich docelowo korzystał na zasadzie wyłączności.</p> <p>C) Umowa licencyjna oprogramowania licencyjnego musi zapewniać możliwość złożenia ponownych zamówień na dowolną ilość licencji w ramach danej umowy licencyjnej przez przynajmniej rok od daty jej podpisania.</p>
LIC 8	<p>Wszystkie udzielone licencje muszą pozwalać na swobodne przenoszenie pomiędzy serwerami/stacjami roboczymi (np. w przypadku wymiany serwera/stacji roboczej); wymaganie to nie dotyczy systemu operacyjnego na stacje robocze.</p>

	Licencje przeznaczone do użytku w SeUI muszą uwzględniać prawo do wykorzystania w ramach środowiska wirtualnego.
LIC 9	Licencjonowanie (dla oprogramowania licencyjnego podmiotów trzecich) musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych w okresie przynajmniej 5 lat od dnia dokonania odbioru końcowego.
	<b>Licencje na potrzeby SeUI</b>
LIC 10	Licencje na potrzeby SeUI będą udzielone w taki sposób i w takim zakresie, aby wystarczyły dla zapewnienia prawidłowego funkcjonowania Systemu PSeAP w okresie 5 lat od dokonania odbioru końcowego - z właściwą wydajnością i pojemnością, zakładając zwiększanie w tym okresie liczby usług dostępnych online oraz liczby użytkowników tych usług (klientów urzędu). Wymagana jest możliwość płatnego lub bezpłatnego pozyskania rozszerzeń w trybie przyrostowym (np. w przypadku zwiększenia liczby użytkowników w jednostkach, zwiększenia zasobów sprzętowych obsługujących System PSeAP).
LIC 11	Licencje na potrzeby SeUI muszą umożliwiać przyłączanie do Portalu e-Usług oraz CPI dodatkowych jednostek samorządu terytorialnego lub jednostek podległych z terenu województwa podkarpackiego, przy czym w zakresie oprogramowania licencyjnego podmiotów trzecich dopuszcza się możliwość płatnego zakupu rozszerzeń dla dodatkowych użytkowników z innych podmiotów, które nie są Partnerami Projektu.
LIC 12	W przypadku, gdy graficzny edytor formularzy jest oprogramowaniem licencyjnym, licencjonowanym na użytkownika, liczba udzielonych licencji musi być równa sumie administratorów lokalnych u poszczególnych Partnerów Projektu, wg załączniku nr 2 do OPZ oraz administratorów centralnych w Centrum Przetwarzania Danych. Licencje muszą obejmować administratorów u wszystkich Partnerów, także z tych podmiotów, którzy nie wdrażają SEOD w ramach Projektu.
LIC 13	Licencje pozwalają na uruchomienie instancji produkcyjnej, testowej oraz szkoleniowej SeUI (instancje testowa i szkoleniowa o pełnej funkcjonalności, na infrastrukturze wirtualnej, przy czym struktura uprawnień i baza użytkowników muszą być analogiczne, jak w instancji produkcyjnej).
	<b>Licencje na potrzeby SEOD</b>
LIC 14	Szczegółowy wykaz udzielonych licencji znajduje się w załączniku nr 1 do OPZ
LIC 15	System musi umożliwiać dołączanie dodatkowych stanowisk (zwiększanie liczby Użytkowników) lub udzielona zostanie licencja otwarta dla Partnerów Projektu.,

	tzn. dająca możliwość wykorzystania SEOD bezterminowo przez dowolną liczbę użytkowników zatrudnionych w instytucji (urzędzie) każdego z Partnerów Projektu.
LIC 16	Wraz z licencjami SEOD, wykonawca dostarczy licencje na wszelkie oprogramowanie pomocnicze niezbędne do prawidłowego funkcjonowania SEOD, w szczególności na oprogramowanie bazodanowe i serwery aplikacyjne, aplikację OCR. SEOD będzie zainstalowany na dostarczonych serwerach i będzie wykorzystywał dostarczone wraz z serwerami oprogramowanie systemu operacyjnego i oprogramowanie podstawowe.
LIC 17	Udzielone licencje na oprogramowanie SEOD powinny umożliwiać zmianę użytkowników korzystających z systemu (zastąpienie jednego użytkownika innym np. w przypadku zmiany pracownika na danym stanowisku) oraz przenoszenie instalacji na różne serwery w obrębie tej samej licencji.
LIC 18	Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, instruktażami stanowiskowymi eksploatacją systemów, Zamawiający wymaga oferty zawierającej licencje pochodzące od jednego producenta, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.
LIC 19	Wymagane jest zapewnienie możliwości korzystania z kopii zamiennych (możliwość kopiowanie oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych. Wymaganie nie dotyczy systemu operacyjnego dla komputerów PC.
LIC 20	Dostarczone licencje na SEOD i oprogramowanie pomocnicze pozwalają na uruchomienie instancji produkcyjnej, testowej oraz szkoleniowej SEOD (instancje szkoleniowe SEOD u każdego z partnerów Projektu, którzy wdrażają SEOD, ponadto instancje testowe SEOD u 10 Partnerów – uczestników pilotażu, dodatkowo po jednej instancji testowej i szkoleniowej SEOD w CPD).
	<b>Inne</b>
LIC 21	Wykonawca zapewni subskrypcję bazy wirusów w dostarczonym oprogramowaniu antywirusowym przez 5 lat od dnia dokonania odbioru końcowego.

## **17 Inne dokumenty do opracowania przez Wykonawcę.**

Wykonawca musi przygotować wzory i rekomendacje w zakresie niezbędnej dokumentacji do wdrożenia systemu PSeAP:

- I) rekomendacje w zakresie zmian w polityce bezpieczeństwa dla Partnerów Projektu
- II) propozycję wzoru zarządzenia, które będzie wprowadzać system EZD jako podstawowy system prowadzenia czynności kancelaryjnych zgodnie z rozporządzeniem w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. Zarządzenie to powinno także m.in.:
  - a) wskazywać wyjątki niepodlegające systemowi EZD,
  - b) wskazywać sposób postępowania ze sprawami niezakończonymi,
  - c) zawierać listę rodzajów przesyłek, dla których nie wykonuje się odwzorowań cyfrowych i parametry graniczne,
  - d) wskazywać maksymalną wielkość przesyłki przekazywanej na informatycznym nośniku danych, którą włącza się bezpośrednio do SEOD (zgodnie z przepisami prawa).
  - e) wskazywać sposób postępowania ze sprawami prowadzonymi w poprzednio użytkowanym elektronicznym systemie obiegu dokumentów, jeśli jednostka taki posiadała.



## 18 Szkolenia

- I) Wykonawca zobowiązany jest do przeprowadzenia szkoleń dotyczących:
- a) Dokument elektroniczny i podpis elektroniczny w administracji publicznej Technologie, prawo, organizacja pracy, archiwizacja;
  - b) Uwarunkowania prawne świadczenia e-usług publicznych
  - c) Ścieżki obiegu dokumentów - notacja, modelowanie, określanie warunków
  - d) Platforma ePUAP - podstawy prawne, funkcjonalność, dodawanie usług
  - e) Organizacja pracy w urzędzie po wprowadzeniu systemu EZD.
- II) Wykonawca przed rozpoczęciem szkoleń przedstawi Zamawiającemu do zatwierdzenia szczegółowy plan szkoleń.
- III) Wykonawca zobowiązany jest do przeprowadzenia szkoleń zgodnie z niżej zamieszczonymi wymaganiami.

<b>Wymagania dotyczące szkoleń</b>	
<b>Wymaganie</b>	
SZKO 1	<p>Szkolenia odbywać się będą zgodnie z ww zakresem i w terminie uzgodnionym z Zamawiającym przy założeniu, iż:</p> <ul style="list-style-type: none"> <li>A) Łączna liczba szkoleń musi wynieść minimum 750 osobodni</li> <li>B) Grupa szkoleniowa nie będzie liczyć więcej niż 15 osób.</li> </ul> <p>Wykonawca zobowiązany jest zapewnić:</p> <ul style="list-style-type: none"> <li>C) salę szkoleniową na terenie Rzeszowa, Krosna, Przemyśla oraz Tarnobrzega.</li> <li>D) odpowiednie do przeprowadzenia szkolenia wyposażenie (stacje robocze, rzutnik, itp.).</li> <li>E) catering- bufet kawowy</li> </ul>
SZKO 2	<p>Szkolenia dotyczące tematyki wymienionej w punkcie 1 A- 1 C muszą być prowadzone w formie wykładów – min. 50 % ogólnego czasu szkoleń, oraz ćwiczeń - min. 50 % czasu ogólnego szkoleń.</p> <p>Pozostałe szkolenia mogą być prowadzone w formie wykładu.</p>
SZKO 3	<ul style="list-style-type: none"> <li>A) Przed rozpoczęciem szkolenia Wykonawca zapewni każdemu uczestnikowi szkolenia komplet materiałów szkoleniowych. Materiały te należy przekazać do siedziby Zamawiającego minimum 14 dni przed planowanym szkoleniem.</li> <li>B) Materiały szkoleniowe powinny zostać dostarczone w formie papierowej i elektronicznej.</li> <li>C) C) Materiały szkoleniowe muszą obejmować całość zagadnień dotyczących zakresu merytorycznego szkolenia.</li> </ul>

SZKO 4	Na początku każdego dnia szkoleniowego Wykonawca sporządzi listę obecności. Udział uczestnika w szkoleniu w danym dniu ma zostać potwierdzony jego podpisem.
SZKO 5	Wykonawca po zakończonym szkoleniu przygotowuje Raport z przeprowadzonego szkolenia.