SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA:

„Dostawa sprzętu komputerowego oraz oprogramowania niezbędnego do realizacji e-Usług wraz z usługą wdrożenia, integracji i szkolenia"

Załącznik nr 2

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

(SzOPZ)

Jonkowo, 31 maja 2019 r.

Spis treści

Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (SzOPZ) w zakresie dostawy i wdrożenia sprzętu oraz oprogramowania służącego uruchomieniu i zabezpieczeniu działania e-Usług w Urzędzie Gminy Jonkowo. Prezentowany poniżej ogólny opis organizacji serwerowni stanowi jedynie zarys całego rozwiązania – Wykonawca może zaproponować swoją wersję organizacji serwerowni o ile proponowane rozwiązanie gwarantowało będzie wyższy poziom bezpieczeństwa i lepsze wykorzystanie mocy obliczeniowej serwerów fizycznych przy czym nie może udostępniać mniejszej szybkości działania. Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne wymagania stawiane oferowanym urządzeniom i oprogramowaniu.

Ogólny zarys projektu

Celem projektu jest wdrożenie nowoczesnych i bezpiecznych e-Usług w Gminie. W tym celu wszystkie obecne i nowe systemy oraz usługi muszą zostać uruchomione w trybie wysokiej dostępności (HA). Aby sprostać temu wymogowi w Gminie zostaną zainstalowane nowe serwery z usługami wirtualizacji i zabezpieczeniami (niezależnym zasilaniem bateryjnym (UPS) oraz urządzeniem typu UTM). Wszystkie nowe i obecne usługi zostaną uruchomione w środowisku wirtualnym w trybie HA.

Fizycznym miejscem instalacji e-Usług będzie lokalizacja główna.

Aby usługi elektroniczne świadczone były w sposób bezpieczny, serwerownia zostanie wyposażona w zasilanie awaryjne UPS, oraz urządzenie typu UTM zabezpieczające ruch sieciowy pomiędzy petentami i placówką oraz gwarantującymi ciągłość dostępności e-Usług.

Niniejszy Przedmiot Zamówienia podzielony jest na następujące zakresy:

Lp.	Opis prac wykonanych w ramach zakresu	Maksymalny czas realizacji
1	Dostawa sprzętu i oprogramowania systemowego.	45 dni od dnia podpisania umowy
2	Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego.	
3	Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym sprzętem.	14 dni od momentu dostarczenia sprzętu
4	Dostawa i wdrożenie systemu Elektronicznego Obiegu Dokumentów	Do zakończenia terminu realizacji zamówienia
5	Dostawa i wdrożenie Portalu e-Usług wraz z formularzami elektronicznymi	Do zakończenia terminu realizacji zamówienia
6	Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym	Do zakończenia terminu realizacji zamówienia

	oprogramowaniem (m.in.: EOD, Portalu eUsług).	
Zakres 7	Przygotowanie oraz dostarczenie dokumentacji projektowej i powykonawczej.	Min. na 7 dni przed planowanym terminem odbioru
Zakres 8	Świadczenie usług serwisowych w ramach gwarancji i rękojmi w ramach całości dostarczonego rozwiązania (zgodnie z ofertą)	Min 36 miesięcy[1]

Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

1. Dysfunkcja – zbiorcze określenie dla nieprawidłowości rozumianych jako niezgodność z Dokumentacją lub też uciążliwość w pracy z Systemem.
2. Kategoria Dysfunkcji - kategoria, do której kwalifikowane jest Zgłoszenie Serwisowe dotyczące Dysfunkcji. Opisane szczegółowo w Załączniku nr 3 do Umowy.

Prace Serwisowe - działania Wykonawcy mające na celu realizację Zgłoszenia Serwisowego.

Naprawa – modyfikacja Systemu usuwająca Dysfunkcję Systemu.

Obejście - tymczasowe rozwiązanie pozwalające na prawidłowe wykorzystanie oprogramowania bez usuwania wykrytego błędu przy zachowaniu integralności bazy danych.

Realizacja Zgłoszenia Serwisowego - zakończenie Prac Serwisowych, w wyniku których przywrócono Stan Funkcjonalności.

Analiza – dokumenty opracowane przez Wykonawcę, mające na celu doprecyzowanie sposobu realizacji wymagań Zamawiającego, zasad i metod realizacji Umowy oraz wskazanie i szczegółowe opisanie Produktów;

Backup – wykonanie kopii bezpieczeństwa danych pozwalających na odtworzenie i przywrócenie Bazy Danych i Systemu po wystąpieniu awarii w przypadku utraty lub uszkodzenia oryginalnych danych; jakość odtworzonych danych powinna być dostosowana do ustalonego uprzednio poziomu ryzyka, który poniesie Zamawiający (poziom ryzyka determinuje cykliczność wykonywania backup'ów).

12. Baza Danych – zbiór wszystkich danych zewidencjonowanych za pomocą Systemu.
13. Czas Roboczy – czas pracy liczony w Dni Robocze, w którym świadczona jest pomoc telefoniczna przy eksploatacji Systemu.
14. Dzień Roboczy – dzień kalendarzowy od poniedziałku do piątku z wyłączeniem świąt i dni ustawowo wolnych od pracy.
15. Dokumentacja – dokument papierowy lub elektroniczny opisujący System i zasady użytkowania Systemu. Wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy.
16. Godziny robocze – czas pracy liczony w Dni Robocze w godzinach 7:30 – 15:30.

[1] Na całość rozwiązania od momentu podpisania ostatniego Protokołu Odbioru Końcowego Zakresów od 1 do 8 – termin zgodni z ofertą.

17. Konsultant – osoba fizyczna posiadająca odpowiednie kwalifikacje uprawniające do realizowania Serwisu.
18. Pomoc Telefoniczna – świadczenie konsultacji telefonicznej dotyczące szeroko pojętej eksploatacji Systemu.
19. Procedura – schemat postępowania w jaki winien być realizowany określony fragment Przedmiotu Umowy.
20. Publikacja – udostępnienie Systemu zawierającego zmienioną funkcjonalność.
21. Serwer – sprzęt komputerowy, na którym zainstalowana jest baza danych lub aplikacje wykorzystywane przez System.
22. Serwis – usługa o charakterze technicznym, organizacyjnym, doradczym i szkoleniowym, przeznaczona do zapewnienia stabilnej pracy Systemu.
23. Stan Funkcjonalności - stan Systemu, w którym nie występują Dysfunkcje.
24. Upgrade – nowa wersja Systemu związana ze stworzeniem nowej funkcjonalności.
25. Update – aktualizacja Systemu w wyniku zmian przepisów, związanych bezpośrednio i pośrednio z systemem ochrony zdrowia, w zakresie tej samej wersji Systemu.
26. Wdrożenie – opisane Umową świadczenia Wykonawcy mające na celu uruchomienie systemu serwerów wirtualnych w trybie HA.
27. Wersja – okresowa Publikacja Systemu uwzględniająca Naprawy i zmiany dokonane w okresie od poprzedniej Publikacji Systemu. Wydanie Wersji obejmuje również opis nowej Funkcjonalności Systemu.
28. Zgłoszenie Serwisowe – Dysfunkcja, o której Wykonawca został powiadomiony drogą mailową.
29. Administrator - Użytkownik konfigurujący i zarządzający Systemem i Infrastrukturą.
30. Architektura systemu teleinformatycznego – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami.
31. Czas dostarczenia rozwiązania - Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Rozwiązania Zastępczego.
32. Dostępność – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym .
33. Integralność – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony .
34. Kierownik Projektu Wykonawcy (KPW) – Osoba ze strony Wykonawcy upoważniona do bezpośredniej koordynacji zadań objętych umową. Do zadań Kierownika Projektu Wykonawcy należy m.in. podpisywanie dokumentów w zakresie Protokołów Odbioru Zadań, Protokołów Odbioru Końcowego.
35. Kierownik Projektu Zamawiającego (KPZ) - Osoba ze strony Zamawiającego upoważniona do bezpośredniej koordynacji zadań objętych umową. Do zadań Kierownika Projektu Zamawiającego należy m.in. podpisywanie dokumentów w zakresie Protokołów Odbioru Zadań, Protokołów Odbioru Końcowego.
36. Moduł systemu – kompletny zestaw narzędzi informatycznych obejmujących wszystkie warstwy architektury systemu, który dostarcza aplikację przeznaczoną dla użytkownika końcowego do realizacji określonych dziedzin działalności Zamawiającego.

37. Oprogramowanie standardowe – Każde oprogramowanie niezbędne do działania Systemu.
38. Portal Usług Elektronicznych – portal udostępniający usługi elektroniczne dostarczane przez System dla użytkowników wewnętrznych i zewnętrznych
39. PKI – Infrastruktura Klucza Publicznego
40. Rozwiązanie zastępcze - proponowane przez Wykonawcę rozwiązanie tymczasowe, usuwające lub niwelujące czasowo do akceptowalnego poziomu skutki wystąpienia Wady, wprowadzone do czasu usunięcia Wady.
41. System – Łączne określenie dla oprogramowania i sprzętu – występującego u Zamawiającego, objętego wdrożeniem oraz umową serwisową z Wykonawcą, bez względu na nazwę handlową. Obejmujący platformę systemowo-sprzętową, oprogramowania aplikacyjne oraz inne oprogramowanie niezbędne do działania e-Usług realizowanych w niniejszym zamówieniu dostarczanych przez Wykonawcę.
42. System Elektronicznego Obiegu Dokumentów – (System Elektronicznego Zarządzania Dokumentami lub EOD lub EZD) – określenie systemu informatycznego do zarządzania obiegiem zadań oraz dokumentów działającego w oparciu o mechanizmy typu workflow
43. System zewnętrzny - Każdy System informatyczny niebędący przedmiotem Zamówienia a oddziaływujący na przedmiot zamówienia.
44. Usługi elektroniczne (eUsługi) – usługi, których świadczenie odbywa się za pomocą Internetu, jest zautomatyzowane (może wymagać niewielkiego udziału człowieka) i zdalne. Od usługi w ujęciu tradycyjnym, eUsługę odróżnia brak udziału człowieka po drugiej stronie oraz świadczenie na odległość.
45. Użytkownik - Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło.
46. Web Service - Usługa sieciowa dostarczająca określoną funkcjonalność poprzez sieci Internet, niezależnie od platformy sprzętowej i implementacji.
47. Wykonawca – wybrany w drodze zamówienia publicznego podmiot realizujący niniejszy przedmiot zamówienia.
48. Zamawiający – Gmina Jonkowo
49. Zdalny dostęp – możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.
50. SZBI – System Zarządzania Bezpieczeństwem Informacji.
51. ASI – Administrator Systemów Informatycznych u Zamawiającego.

Wymagania ogólne

Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).

System musi być zbudowany w architekturze wysokiej dostępności (HA).

System musi umożliwiać definiowanie dowolnej ilości użytkowników.

System musi posiadać graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po dowolnych kryteriach. Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, itp. dla których wymogi minimalne co do posiadanych interfejsów zostały opisane odrębnie.

System musi gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych.

System musi pracować w środowisku sieciowym i posiadać wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników bez ograniczeń na ich liczbę.

System musi posiadać mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych.

System musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji.

Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne okresowe [np. na aktualizację systemu zabezpieczeń] na min. okres zaoferowanej gwarancji na urządzenie na którym licencje są instalowane; nośniki instalacyjne, instrukcje.

Minimalny okres gwarancji - 36 msc. - dotyczy wszystkich elementów systemu – o ile w specyfikacji i/lub ofercie nie wyszczególniono inaczej (np. baterie UPS).

Zakres 1 – Dostawa sprzętu i oprogramowania systemowego

Poniżej przedstawiono parametry minimalne jaki dostarczany sprzęt musi spełniać. W przypadku gdy do realizacji Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nie ujęte w poniższym zestawieniu Wykonawca musi go dostarczyć i wykazać w wykazie asortymentowo-cenowym.

Serwery

Serwery aplikacyjne i bazodanowe – 2 szt.

Parametr	Wymagania minimalne
Obudowa	RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia), maksymalnie 2U
Procesor	Min. jeden procesor. Płyta główna wspierająca zastosowanie procesorów min. do 28 rdzeniowych. Min. 8-rdzeniowy[2] klasy x86 - 64 bity, osiągające w testach w testach PassMark – wynik nie gorszy niż 11700 punktów. Wynik testu musi być opublikowany na stronie cpubenchmark.net
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5" System wirtualizacji zainstalowany na nośniku bez konieczności użycia dysków twardych. Wykonawca musi dostarczyć nośniki danych (min. 8GB każdy). Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.
Kontroler	Serwer wyposażony w min. 2-portowy kontroler sprzętowy SAS służący do podłączenia macierzy.
Pamięć operacyjna	min. 128 GB DIMM DDR4 w modułach o pojemności min. 8GB każdy z możliwością rozbudowy do min. 1,5TB.
Sloty rozszerzeń	2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16
Interfejsy sieciowe	Minimum 4 porty eth 100/1000 Mb/s RJ-45 z wsparciem dla PXE.
Karta graficzna	Zintegrowana karta graficzna
Porty	Min.: 4 x USB (co najmniej jeden z przodu obudowy); 1x VGA;
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy min. 500W i max. 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug. Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia do 40°C, zgodność ze standardem ASHRAE Class A4
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe

[2] Parametr ważny z uwagi na docelowe wykorzystanie serwera

	• wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez – dedykowany port RJ45 – przez współdzielony port zintegrowanej karty sieciowej serwera • dostęp do karty możliwy – z poziomu przeglądarki webowej (GUI) – z poziomu linii komend – poprzez interfejs IPMI 2.0 • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz SNMP • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • funkcja zdalnej konsoli szeregowej - przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • zdalna aktualizacja oprogramowania (firmware) • możliwość równoczesnej obsługi przez min. 2 administratorów • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DHCP) Rozwiązanie sprzętowe posiadające dedykowany port RJ45.
Wsparcie dla systemów operacyjnych i wirtualizacyjnych	Min.: Microsoft Windows Server 2016, Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server, VMware ESXi 6.5 i nowsze
Gwarancja	Z czasem reakcji NBD. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie, potwierdzające pochodzenie oferowanego urządzenia z oficjalnego kanału dystrybucyjnego producenta.

Macierz dyskowa

Macierz dyskowa przechowywująca dyski maszyn wirtualnych i dane użytkowników – 1 szt.

Parametr	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U.
Przestrzeń dyskowa	Macierz musi udostępniać minimum 9 TB przestrzeni RAW zbudowanej w oparciu o minimum 7 dysków w technologii SAS o prędkości obrotowej min. 10k obr/min; min. 500 GB przestrzeni RAW zbudowanej w oparciu o min. 2 dyski SSD.
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 150 dysków twardych.
Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i NLSAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NLSAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5 oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Oferowana konfiguracja dyskowa musi zawierać min. rekomendowaną przez producenta ilość dysków spare.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe poprzez interfejsy SAS. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 4 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM – nie zezwala się użycia dysków SSD do tego rodzaju cache. Pamięć zapisu musi być mirrorowana pomiędzy kontrolerami dyskowymi. Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 12 miesięcy.
Interfejsy	Macierz musi posiadać, co najmniej 4 aktywne porty SAS 12 Gb/s.
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i konsoli CLI. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami	Macierz musi umożliwiać zdefiniowanie, co najmniej 200

dyskowymi oraz dyskami logicznymi	wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Kopie pełne i migawkowe	Macierz musi umożliwiać dokonywania na żądanie min. 200 tzw. migawkowych kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą relokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są

	dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, Vmware. Macierz musi posiadać wsparcie dla różnych systemów klastrowych, co najmniej Microsoft Cluster. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek – jeśli wymagane. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych lub wielu serwerów. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Wraz z macierzą mają zostać dołączone kable SAS umożliwiające podłączenie serwerów - w ilości min. 4 szt.
Gwarancja	Gwarancja producenta w miejscu instalacji z czasem reakcji NBD.

Serwer backupu

Serwer wykonywania i przechowywania kopii bezpieczeństwa – 1 szt.

Parametr	Wymagania minimalne
Procesor	Dedykowany do obsługi urządzeń typu NAS z obsługą wirtualizacji maszyn x86 (34 i 64b).
Obudowa	Rack, max. 2U, szyny montażowe w zestawie
Pamięć RAM	min. 16 GB RAM

Interfejsy sieciowe	Min: 4 x Gigabit
Porty	Min. 1x USB 3.0
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Wspierane systemy operacyjne	Microsoft Windows Server 2016, Linux, Vmware
Protokoły	CIFS, AFP, NFS, FTP, iSCSI, Telnet, SSH, SNMP
Wirtualizacja	Certyfikat zgodności Vmware Ready, Windows Server 2016 Certified. możliwość uruchomienia maszyn wirtualnych bezpośrednio na macierzy bez konieczność posiadania zewnętrznych wirtualizatorów.
Szyfrowanie	Szyfrowanie ze wsparciem sprzętowym całych woluminów oraz wybranych udziałów sieciowych
iSCSI	Wbudowany inicjator i target iSCSI
Replikacja	Replikacja między urządzeniami w czasie rzeczywistym
Kontroler domeny	Możliwość podłączenia do kontrolera domeny Microsoft
Liczba iSCSI LUN	Min. 64
Liczba kont użytkowników	Min. 200
Liczba grup	Min. 100
Liczba udziałów	Min. 100
Liczba jednoczesnych połączeń	Min. 500
Zasilanie	Redundantne 2x max. 400W
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
Dyski zainstalowane	4 dyski o pojemności: min. 8TB każdy Pamięć podręczna: min. 128MB Prędkość obrotowa: min. 7200RPM MTBF: min. 2 000 000 h Maks. wew. szybkość przesyłania: min. 200 MB/s

Zasilanie awaryjne – UPS

Zasilacz UPS do serwerowni -1 szt.

Parametr	Wymagania minimalne
Moc znamionowa	Min. 3000 VA
Obudowa	Do montażu w szafie Rack 19”
Maksymalna wysokość UPS	Maks. 3U (bez dodatkowych modułów bateryjnych)
Maksymalna głębokość	Maks. 700 mm
Zakres napięcia wejściowego	Min. 190–260 V
Napięcie nominalne wyjściowe	220/230/240 V

Gniazda wyjściowe	Min. 4 szt. IEC-320-C13 (10A) i min. 1 szt. IEC-320-C19 (16A)
Sprawność	Min. 90%
Częstotliwość wyjściowa	50/60 Hz +/- 0,1% (autodetekcja)
Czas podtrzymania dla obciążenia 100%	Min. 20 minut
Czas podtrzymania dla odciążenia 50%	Min. 40 minut
Obsługa dodatkowych baterii	do 4 modułów bateryjnych o wysokości max 4U każdy
Zarządzanie akumulatorami	System ładowania nieciągłego baterii z kompensacją temperatury, automatyczne sprawdzanie akumulatorów, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie dodatkowych zewnętrznych modułów bateryjnych, wymiana akumulatorów „na gorąco" bez konieczności wyłączania podłączonych urządzeń.
Interfejs użytkownika	Wyświetlacz LCD (informacje o statusie i pomiarach UPS, możliwość pomiaru zużycia energii w kWh)
Standardowe gniazda komunikacyjne	Karta sieciowa + 1 x styki przekaźnikowe + 1 mini złącze zdalnego zał./wył. i wyłączenia
Zdalne zarządzanie	• Kompatybilność z HTTP, SNMP, SMTP, SSH, TLS • Konfigurowalne akcje zawierające automatyczne zamykanie systemów w przypadku przedłużających się przerw w zasilaniu • Powiadamianie e-mailowe o alarmach • Kompatybilność z SNMPv3 i IPv6 • Konfigurowalne automatycznie powiadamiania e-mail w odpowiedzi na alarmy UPS oraz przesyłanie raportów okresowych • Sterowanie załączaniem i wyłączaniem UPS poprzez przeglądarkę internetową • Pomiar wilgotności i temperatury z opcjonalnym czujnikiem monitorowania środowiska • Automatyczne ustawienia daty i godziny poprzez serwer NTP • Zabezpieczenie hasłem • Transmisja szyfrowana • Zapis dziennika zdarzeń w pamięci trwałej
Poziom hałasu	Max. 64 dB
Bezpieczeństwo, zakłócenia elektromagnetyczne	IEC/EN 62040-1, IEC/EN 62040-2
Certyfikaty	CE, raport CB, TÜV
Gwarancja na akumulatory	Min. 2 lata
Oprogramowanie do zarządzania i monitoringu UPS	Pakiet oprogramowania kompatybilny z MS Windows Server oraz RedHat Linux, włącznie z oprogramowaniem wirtualizacyjnym, takim jak Vmware i Hyper-V. Oprogramowanie musi mieć możliwość rozbudowy o funkcję zawieszania działania niekrytycznych maszyn wirtualnych, przenoszenia maszyn wirtualnych lub łagodnego wyłączania systemu w przypadku

	długotrwałej przerwy w dostawie energii.
Wyposażenie dodatkowe	Zestawy gniazd wyjściowych PDU o prądzie nominalnym 16A podłączane do gniazda wyjściowego w zasilaczu awaryjnym UPS, obudowa 1U do montażu w szafie Rack (19") z możliwością montażu w wielu położeniach z min. 12 szt. gniazd IEC-320-C13 (10A) i 1 szt. IEC-320-C19 (16A) (z 2 bezpiecznikami nadprądowymi), z zaciskami zabezpieczającymi przed przypadkowym wyciagnięciem kabla zasilającego na gniazdkach wejściowych i wyjściowych. Czujnik monitorowania środowiska UPS umożliwiający zdalne monitorowanie temperatury, wilgotności i dwóch urządzeń stykowych podłączany do karty sieciowej SNMP.

Stanowiska robocze stacjonarne

Komputer – 5 szt.:

Parametr	Wymagania minimalne
Procesor/Chipset	Wielordzeniowy, min. 10000 pkt. w teście PassMark - CPU Mark
Karta graficzna	min. 400 pkt. w teście PassMark - G3D Mark
System operacyjny	Umożliwiający uruchomienie systemów dziedzinowych Zamawiającego bez użycia wirtualizacji w wersji pozwalającej na zarządzanie systemem za pomocą domeny Active Directory.
Oprogramowanie biurowe	Oprogramowanie biurowe zawierające, min: arkusz kalkulacyjny, edytor tekstu, program do tworzenia prezentacji. Dostarczony pakiet musi w 100% obsługiwać wszystkie funkcje/opcje dokumentów tworzonych w posiadanym przez Zamawiającego pakiecie MS Office 2013/2016. Licencja na oprogramowanie nie może ograniczać czasowo ani funkcjonalnie dostarczonego oprogramowania po okresie udzielonej gwarancji.
Pamięć masowa	Min. 250GB SSD, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. Łącznie w komputerze musi być zainstalowane min. 1 TB przestrzeni dyskowej. Dodatkowa przestrzeń dyskowa może być zrealizowana przez dysk talerzowy.
Napęd optyczny	min. DVD-RW
Pamięć RAM	min. 8GB
Sieć	10/100/1000 Ethernet
Porty wbudowane	min. 6 USB (w tym co najmniej 2 porty 3.0), 1 RJ45, 1 VGA, 1x DisplayPort lub HDMI – zgodny z zaoferowanym monitorem, audio jack.
Akcesoria w zestawie	Klawiatura i mysz przewodowe.
Moc pobierana	<220W
Zasilanie:	220-240V @ 50Hz
Wymiary max. obudowy komputera (szer. x głęb. x wys)	100mm x 300mm x 300mm

Waga komputera	max. 7kg
Certyfikaty	TÜV-GS, EN 60950 RF Interference: FCC Class B, Ergonomics CE, VCCI, RoHS Compliant
UWAGA	Wraz z zestawami należy dostarczyć: • Kabel zasilający, • klawiaturę i mysz optyczną – przewodowe. Oferowana seria komputera musi posiadać certyfikat potwierdzający poprawną współpracę oferowanego komputera z zaoferowanym systemem operacyjnym.

Monitor – 5 szt.:

Parametr	Wymagania minimalne
Ekran	min. 23 cali, Full HD 1920 x 1080 @ 60 Hz, proporcje: 16:9 lub zbliżone, Powłoka antyodblaskowa/matowa
Jasność	min. 220 cd/m^2
Kontrast	min. 1000:1 (statyczny)
Złącza	min. 1 złącze cyfrowe (DP lub HDMI lub DVI) zgodne ze złączem karty graficznej oferowanego komputera
Podstawka	z możliwością pochylenia o min. +10°
Zasilanie	Max 30W, z sieci 240VAC
UWAGA	Wraz z zestawami należy dostarczyć: • kabel odpowiedni do podłączenia monitora z komputerem, • kabel zasilający,

Zamawiający dopuści dostarczenie komputera typu AiO spełniającego łącznie parametry komputera i monitora.

Drukarka etykiet – 2 szt.

Parametr	Minimalne wartości parametru
Dostępne interfejsy:	min. USB, Ethernet (LAN)
Rozdzielczość druku [dpi]:	min. 200
Rodzaj druku:	termiczny
Maks. prędkość druku [mm/s]:	min. 100
Wymiary [mm] WxHxL:	max: 255 x 255 x 255
Min. szerokość etykiet [mm]:	max. 30
Szerokość druku [mm]:	min. 100
Maks. długość druku [mm]:	min. 200
Zasilanie:	AC: 230V / 50 Hz

Czytniki kodów kreskowych – 2 szt.

Parametr	Minimalne wartości parametru
Rodzaje interfejsu:	min. USB, RS-232, PS/2 (Keyboard Wedge); wymagany min. kabel USB
Typ skanera:	Imager 1D/2D
Odczytywane kody kreskowe:	min: Code 39, Code 128, Code 93, Codabar/NW7, Code 11, MSI Plessey, UPC/EAN, Interleaved 2 z 5, koreański 3 z 5, GS1 DataBar, Base 32, PDF417, TLC-39, Aztec, DataMatrix, MaxiCode, QR Code, MicroQR
Zasięg odczytu:	min. 0,4m
Szybkość skanowania:	min. 70 cm/sek.
Sygnalizacja odczytu:	dźwiękowa i świetlna
Odporność na upadki:	min. do 1,5m
Norma szczelności:	Zabezpieczony przeciwko działaniu kurzu (IP42)
Zasięg pracy od bazy komunikacyjno-ładującej:	min. 5m – komunikacja radiowa.

Skaner (USB) – 1 szt.

Parametr	Minimalne wartości parametru
Typ skanera	Dokumentowy (Duplex) A4
Źródło światła	LED
Podawanie papieru	ADF min. 50 arkuszy
Gramatura papieru	min. 30 - 400 g/m^2
Optyczna rozdzielczość	min. 600 dpi
Rozdzielczość wyjściowa	min. od 100 do 600 dpi
Rozmiar dokumentów	Min. od 90x90 mm, do 216 mm x 355 mm
Skanowanie długich dokumentów	Do min. 5 m
Prędkość skanowania	min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 200 dpi)
Głębia koloru	min. 16 bit wyjściowe
Skala szarości	min. 8 bit wyjściowe
Interfejs	min. USB 2.0
Zasilanie	240 V AC, 50Hz
Sugerowana obciążalność dzienna	min. 4000 stron
Obsługiwane systemy operacyjne	Min. Windows 10
Wykrywanie błędów	Czujnik ultradźwiękowy
Wymiary urządzenia	Max. 320 mm x 220 mm x 250 mm (szerokość x głębokość x wysokość)

Przełącznik sieciowy

24 port – 2 szt.

Parametr	Wymagania minimalne
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn
Porty	Minimum 24 porty GigabitEthernet w standardzie BaseT minimum 2 zintegrowane porty 10Gb Ethernet SFP+, minimum 2 porty do łączenia przełączników w stos, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232 lub USB.
Wydajność przełącznika	minimum 32000 adresów MAC switch fabric capacity min. 120 Gbps forwarding rate min. 90 Mbps pamięć flash min. 4GB bufor pamięci dla pakietów minimum 4MB pamięć procesora minimum 1GB obsługa minimum 4000 wirtualnych sieci możliwość połączenia w stos do 8 urządzeń tego samego typu Wsparcie dla agregacji LACP (802.3ad)
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ad Link Aggregation with LACP 802.3az Energy Efficient Ethernet (EEE) 802.3x Flow Control ANSI LLDP-MED (TIA-1057) Funkcjonalność warstwy 3 : 2453 RIPv2 QoS: 2474 DiffServ Field 2475 DiffServ Architecture 2597 DiffServ Assured Forwarding 2598 DiffServ Expedited Forwarding
Zarządzanie siecią i bezpieczeństwo	1155 SMIv1 1157 SNMPv1 1213 MIB-II 1492 TACACS+ 1493 Managed objects for Bridges MIB 1901 Community-based SNMPv2 1907 SNMPv2 MIB

	1908 Coexistence between SNMPv1/v2 2246 TLS v1 2576 Coexistence between SNMPv1/v2/v3 2578 SMIv2 2579 Textual Conventions for SMIv2 2580 Conformance Statements for SMIv2 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2665 Ethernet-like Interfaces MIB 2674 Extended Bridge MIB 2737 ENTITY MIB 2818 HTTP over TLS 2819 RMON MIB (groups 1, 2, 3, 9) 2856 Text Conv. For High Capacity Data Types 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3411 SNMP Management Framework 3412 Message Processing and Dispatching 3413 SNMP Applications 3414 User-based security model 3415 View-based control model 3416 SNMPv2 3417 Transport Mappings 3418 SNMP MIB 3580 802.1X with RADIUS 4113 UDP MIB 4251 SSH Protocol 4252 SSH Authentication 4253 SSH Transport 4254 SSH Connection Protocol 4419 SSH Transport Layer Protocol 2131DHCP Server
Warunki pracy	- temperatura pracy w zakresie od 0 do 40°C - wilgotność dla trybu pracy do 80%
Funkcjonalność	Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych urządzeń
Certyfikaty i standardy	Zamawiający wymaga aby oferowany przełącznik:

	- posiadał deklarację CE - był zgodny z standardem RoHS
Gwarancja	Gwarancja czasu życia (Limited Lifetime warranty, min. 60 miesięcy) obejmująca: - przełącznik - zasilacze i wiatraki - moduły SFP, SFP+ i QSFP+ - bezterminowy dostęp do nowych wersji oprogramowania

Skaner A1

Skaner – 1 szt.:

Parametr	Wymagania minimalne
Maks. szerokość skanowania	Min. 65 cm
Maks. szerokość dokumentu	Min. 70 cm
Maks. grubość dokumentu	Min. 1 mm
Minimalny rozmiar dokumentu	16 x 16 cm
Tryby skanowania	Min. kolor (24b), skala szarości (8b), monochromatyczny (1b)
Rozdzielczość optyczna	Min. 1200 dpi
Prędkość skanowania	Min. 30 cm/sekundę dla skali szarości 8-bit @200dpi Min. 15 cm/sekundę dla koloru 24-bit @200dpi
Interfejs	Min. USB 3.0
Przestrzeń barwna	RAW, RGB/sRGB
Uwagi	Skaner musi zostać dostarczony wraz z dedykowaną podstawką/szafką umożliwiającą wygodną pracę ze skanerem; wszystkimi kablami umożliwiającymi podłączenie skanera do komputera i zasilania (kabel USB min. 5m – w razie potrzeby można zastosować aktywne przedłużacze USB).

Szafa RACK 42U

Szafa – 1 szt.:

Parametr	Wymagania minimalne
Wysokość	42U
Szerokość całkowita	800 mm
Głębokość całkowita	1200 mm
Szerokość szyn montażowych	Standard 19 cali
Ilość belek nośnych	Dwie pary belek nośnych 19 cali o płynnej regulacji położenia
Wykonanie drzwi przednich	Blaszane, jednoskrzydłowe, perforowane (prześwit ok. 80%) z zamkiem z klamką, możliwość zmiany kierunku otwierania drzwi
Kąt otwarcia drzwi przednich	Min. 180°
Wykonanie drzwi tylnych	Blaszane, perforowane (prześwit ok. 80%) z zamkiem

	trzypunktowym z klamką
Ściągane panele boczne	dwie osłony boczne, pełne z zamkami
Możliwość łączenia szaf	możliwość łączenia szaf w układy szeregowe oraz zabudowy typu Data Box
Otwory kablowe	w płycie dolnej i górnej o szerokości min. 70 mm, wszystkie otwory w zamknięte wyłamywanymi zaślepkami
Stopki poziomujące	Tak
Zestaw przewodów uziemiających	Tak
Numeracja jednostek U na belkach nośnych	Tak
Obciążenie dopuszczalne	Min.1100 kg
Wykończenie powierzchni: szkielet, osłony, drzwi	Malowane farbą proszkową o grubej strukturze
Wykończenie powierzchni: belki nośne, ceowniki	Alucynk
Klasa ochrony	IP 20 zgodnie z normą PN-EN 60529

Zabezpieczenie e-Usług

Firewall – UTM – 1 komplet

Platforma służąca zabezpieczeniu dostępu do systemu eUsług oraz do innych usług zainstalowanych u Zamawiającego, pozwalająca na filtrowanie ruchu z/do internetu do/z sieci LAN. Platforma musi umożliwiać kontrolę w warstwie aplikacji oraz umożliwiać zdalny dostęp do sieci LAN zamawiającego jednostkom zewnętrznym. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca na wezwanie Zamawiającego winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Parametr	Wymagania minimalne
Typ systemu ochrony	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, o zalecanej przez producenta mocy obliczeniowej wystarczającej do zabezpieczenia min. 50 komputerów w sieci LAN oraz minimum 4 aplikacje webowe zainstalowane w infrastrukturze Zamawiającego w trybie HA. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

	1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego
Wymagania systemowe	Obsługa nielimitowanej ilości hostów w sieci chronionej. Obudowa przeznaczona do montażu w szafie RACK. Minimalna liczba i typ interfejsów fizycznych: 10x GE (IEEE 1000Base-T), 2x gniazda SFP, USB do podłączenia modemu 3G/LTE, 1x Console (RJ-45, USB lub DB9) Minimalna liczba i typ interfejsów wirtualnych: 128 (IEEE 802.1Q) Minimalna liczba nowych połączeń na sekundę: 30 000 Minimalna liczba jednoczesnych połączeń: 1 300 000 Minimalna przepustowość Stateful Firewall: 4 000 Mbps Minimalna przepustowość IPS: 450 Mbps Minimalna przepustowość IPSec: 2000 Mbps Minimalna przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: 900 Mbps

	Minimalna przepustowość systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http: 130 Mbps Minimalna liczba równoczesnych tuneli IPSec VPN: 100 Minimalna liczba równoczesnych tuneli SSL VPN: 20 Zintegrowany dysk do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
Zarządzanie i utrzymanie	Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (WebGUI). Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow lub innego oferującego podobne funkcje, System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN
Konfiguracja sieciowa oraz	W zakresie routingu rozwiązanie powinno zapewniać obsługę:

routing	• Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Kształtowanie pasma	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Autoryzacja użytkowników	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Opcje VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych

	zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling.
Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Ochrona i kontrola Web	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Ochrona i kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

	Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Logowanie zdarzeń i raportowanie	Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG
Kontrola Antywirusowa	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze
Certyfikaty	CE, VCCI, ICSA dla SSLVPN, ICSA lub EAL4 dla funkcji Firewall, ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW
Subskrypcje	Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż okres gwarancji.
Gwarancja i wsparcie	Wsparcie techniczne w trybie min 8h/5dni w tygodniu w całym okresie gwarancji. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. Dostarczone rozwiązanie musi zapewniać wysoką dostępność (HA).

Kopie zapasowe

Wykonawca w ramach umowy dostarczy, zainstaluje i wdroży automatyczny system wykonywania kopii bezpieczeństwa zainstalowanych systemów wirtualnych i fizycznych. Wdrożony system kopii bezpieczeństwa musi współpracować w dostarczonym hypervisorem i spełniać następujące parametry:

- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji min. 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych

maszyn wirtualnych wspieranych przez vSphere i Hyper-V

- Oprogramowanie musi być licencjonowanie w modelu "per-CPU" lub „per Serwer". Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczone bajty danych, dodatkowo płatna deduplikacja) nie jest dozwolone
- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi posiadać wbudowane mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
- Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej dwóch pamięci masowych w takiej puli.
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
- Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal, umożliwiający odtwarzanie ASI wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
- Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez ASI poziomy latencji.
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
- Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z

infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji
- Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
- Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc
- Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie
- Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
    - Linux : ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
    - Windows : NTFS, FAT, FAT32, ReFS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 R2 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
- Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
- Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
- Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

System zarządzania i monitorowania infrastruktury serwerów

System zarządzania infrastrukturą wirtualizacji serwerów musi spełniać następujące kryteria:

1. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
2. Pojedynczy klaster może się skalować min. do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
3. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi obsłużyć i wykorzystać procesory fizyczne wyposażone w min 256 logicznych wątków oraz do min. 8 TB pamięci fizycznej RAM.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych min. od 1 do 64 procesorowych.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do min. 4 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć min. do 10 wirtualnych kart sieciowych.
8. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
11. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 10, Debian, CentOS, FreeBSD,.
12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem HTML.
15. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.

16. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
18. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
19. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
20. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
21. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
22. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
23. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
24. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do min. 4000 portów.
25. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
26. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN)

System monitorowania infrastruktury serwerów wirtualnych musi spełniać następujące kryteria:

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware

- System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych:
    - Microsoft Windows 2012 R2
    - Microsoft Windows 2016
    - Microsoft Windows 7 z SP1
    - Microsoft Windows 10
- System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:
    - Microsoft SQL Server 2012 R2
    - Microsoft SQL Server 2014
    - Microsoft SQL Server 2016
- System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej n
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie min. HTML
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- Silnik raportowania powinien być oparty o SQL w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.0, vCenter Server 5.x oraz 6.0 jak również Microsoft Hyper-V 2012 R2i 2016.
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi instalować się na następujących systemach operacyjnych:
    - Microsoft Windows 7 SP1
    - Microsoft Windows 2012 R2
    - Microsoft Windows 10
    - Microsoft Windows 2016

- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów min. do formatów Microsoft Word, Microsoft Excel, PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić 1 godzinę lub krótszy
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach „what-if".
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

Licencje

W ramach postępowania należy dostarczyć wszystkie licencje wymagane do uruchomienia oraz użytkowania dostarczanych urządzeń i serwerów zgodnie z ich przeznaczeniem i niniejszym SIWZ. Licencje terminowe, subskrypcje, abonamenty, itp. muszą pozwalać na użytkowanie każdego elementu Systemu przez okres udzielonej gwarancji od dnia podpisania protokołu odbioru – jeśli dotyczy.

Wykonawca określi ilości i rodzaje licencji wymaganych do realizacji Projektu inne niż wymagane, tj.:

- Serwerowe systemy operacyjne – zgodnie z warunkami licencjonowania do uruchomienia maszyn wirtualnych niezbędnych do realizacji przedmiotu zamówienia (np. jeśli wymagane będą serwery Microsoft Windows Server – należy dostarczyć odpowiednią ilość licencji do uruchamiania maszyn na wszystkich dostarczonych serwerach fizycznych),
- Licencje dostępowe pozwalające na korzystanie z usług systemów Microsoft Windows Server (30 sztuk licencji na urządzenie),
- System kopii bezpieczeństwa (serwery) – zgodnie z warunkami licencjonowania do wykonywania kopii bezpieczeństwa wszystkich zainstalowanych serwerów wirtualnych,
- Systemy bazodanowe – zgodnie z licencjonowaniem, niezbędne do uruchomienia w trybie HA dla wszystkich dostarczanych usług i systemów – zgodnie z wymaganiami dostarczanych systemów (np. Microsoft SQL Server, Oracle, itp.- jeśli wymagane),

- System wirtualizacji – zgodnie z warunkami licencjonowania do uruchomienia nielimitowanej ilości maszyn wirtualnych na wszystkich dostarczonych serwerach,
- System monitorowania infrastruktury serwerowej – zgodnie z licencjonowaniem, do monitorowania wszystkich dostarczanych serwerów.

Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego

Wszystkie dostarczane urządzenia muszą zostać zainstalowane [tj. wypakowane, zmontowane, zamontowane w szafach RACK lub na biurkach, uruchomione i skonfigurowane] w docelowym miejscu pracy [wskazanym przez Zamawiającego] w terminie uzgodnionym z Zamawiającym [miejsce i termin instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń]. Wszystkie opakowania zostaną zutylizowane przez i na koszt Wykonawcy.

Wszystkie urządzenia i systemy operacyjne serwerów muszą być zsynchronizowane z lokalnym serwerem czasu.

Serwery, macierz, firewall, UPS oraz wszystkie inne dostarczone w ramach tego postępowania urządzenia przeznaczone do instalacji w szafie RACK, muszą być zainstalowane w szafie RACK. Wykonawca dostarczy szafę RACK 19" 42U o parametrach minimalnych podanych w poprzednim rozdziale. W ramach prac należy zdemontować obecną szafę RACK i zainstalowane obecnie w szafie urządzenia zamontować w nowej szafie RACK.

Serwery

Na serwerach należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy w możliwie najszybszy sposób. Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia. Wykonawca zaprojektuje i wdroży system backupu min. maszyn wirtualnych.

Macierz dyskowa

Macierz musi zostać zainstalowana w serwerowni. Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób.

Serwer Kopii Zapasowych

Serwer kopii zapasowych musi zostać zainstalowany w serwerowni. Zasoby serwera kopii posłużyć mają do przechowywania dodatkowych kopii bezpieczeństwa systemów zainstalowanych w serwerowni. Serwer musi zostać podłączony do sieci wewnątrz serwerowej.

Zasilanie awaryjne – UPS

Wszystkie dostarczone urządzenia UPS muszą posiadać aktywne karty sieciowe pozwalające na monitorowania za pomocą min.: Interfejsu WEB oraz protokołu SNMP w wersji 2 oraz 3. Wszystkie zasilacze awaryjne muszą zostać skonfigurowane w taki sposób, aby w przypadku zaniku napięcia w sieci energetycznej wysyłana była wiadomość e-mail do ASI oraz aby rejestrowany był ten fakt w centralnym systemie logów lub systemie monitorowania serwerów i usług za pomocą SNMP Trap [włącznie z informacją o przywróceniu napięcia]. Dodatkowo za pomocą SNMP rejestrowane muszą być wszystkie inne zdarzenia mogące mieć wpływ na działanie systemów i ich bezpieczeństwo [np. konieczność wymiany baterii czy przeciążenie]. W systemie zarządzania należy utworzyć dwóch użytkowników z prawami administracyjnymi [jeden dla ASI, jeden dla serwisu]. Jeśli interfejs posiada konto „gościa" należy je wyłączyć. Wszystkie możliwe protokoły

sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepowołanym dostępem. Wszystkie UPSy muszą zostać zainstalowane w szafie RACK w przeznaczony przez producenta do tego celu sposób [np. za pomocą odpowiednich szyn lub uchwytów]. UPS musi zostać podłączony do sieci LAN poprzez dedykowany interfejs zarządzania do odpowiedniego portu na przełączniku sieciowym [odpowiedni vlan!] oraz do dedykowanego obwodu elektrycznego. Jeśli zainstalowana rozdzielnica elektryczna będzie niewystarczająca do zasilania wszystkich urządzeń zainstalowanych w szafie RACK Wykonawca zmodernizuje rozdzielnicę w sposób zalecany przez producenta UPSa zapewniający poprawną pracę wszystkich urządzeń i zgodnie z dobrymi praktykami.

Stanowiska robocze

Konfiguracja urządzeń polegać będzie na:

- wypakowaniu urządzenia z opakowania,
- podłączeniu fizycznym do sieci LAN oraz elektrycznej
- skonfigurowaniu adresu IP na serwerze DHCP,
- konfiguracji interfejsu zarządzania [jeśli posiada], konfiguracji synchronizacji z lokalnym serwerem czasu.

Zabezpieczenie e-Usług

Wykonawca dokona instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.

Wykonawca wdroży [tj. zainstaluje, uruchomi, skonfiguruje i przetestuje] infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerze fizycznym Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem [np. DHCP, DNS, SQL, IIS, SMB, etc.].

Firewall – UTM

W konfiguracji urządzeń muszą zostać włączone min. usługi:

- ochrony przed atakami typu DoS/DDoS, itp.,
- ochrony antywirusowej,
- web filter,
- IDS/IPS,
- Utworzenie konfiguracji serwera VPN.

Instalowane urządzenie musi chronić zainstalowane wewnątrz sieci Zamawiającego serwery aplikacyjne e-Usług [głównie przed atakami typu DoS, sql-injection, itp].

Kopie zapasowe

Wykonawca we współpracy z ASI opracuje politykę kopii bezpieczeństwa uwzględniającą możliwości techniczne po wdrożeniu Projektu. Na podstawie polityki Wykonawca skonfiguruje systemy i usługi do wykonywania kopii bezpieczeństwa zgodnie z harmonogramami. Przetestuje działanie mechanizmu automatycznego wykonywania kopii bezpieczeństwa i po ustalonym z Zamawiającym okresie (np. 30 dni) od uruchomienia harmonogramu oceni skuteczność wdrożonych mechanizmów. W ramach wdrożenia musi zostać dostarczona instrukcja odtwarzania

danych w różnych zakresach [np.: pojedynczy plik, cały katalog, użytkownik wraz z plikami, maszyna, itp.]. Wszystkie kopie muszą być zapisywane min. na serwerze kopii.

Architektura HA dla serwera aplikacji

W celu zapewnienia wysokiej dostępności e-Usług należy uruchomić wirtualne serwery aplikacji w trybie HA. W celu wyeliminowania pojedynczego punktu awarii (jeśli zostanie zastosowany serwer load-balancera) usługa load-balancing'u również musi zostać uruchomiona w trybie HA (np. z wykorzystaniem DNS round-robin). W celu zapewnienia rozliczalności danych w trybie HA muszą zostać uruchomione zarówno serwery load-balancing'u oraz aplikacji jak i e-Usług. Wykonawca może zaproponować inne rozwiązanie gwarantujące równie wysoką dostępność.

Architektura HA dla serwerów bazy danych

Serwery baz danych systemów muszą zostać zabezpieczone na wypadek awarii zarówno serwera wirtualnego jak i fizycznego. Dlatego instancja serwera bazy danych musi zostać uruchomiona w trybie HA. Zamawiający nie stawia wymogu zastosowania konkretnej technologii czy konkretnego rozwiązania, wymaga jedynie spełnienie funkcjonalności w tym zakresie. Podstawowy serwer bazy danych musi zostać skonfigurowany w sposób maksymalizujący szybkość działania systemu bazodanowego [np.: podział dysków na grupy RAID, przeniesienie logów na oddzielne dyski, itp.]. Serwer zapasowy musi się uruchomić najwyżej w ciągu 5 minut i przejąć rolę serwera podstawowego. Po przywróceniu działania serwera podstawowego powinien stać on się serwerem zapasowym lub jeśli będzie oferował lepszą wydajność powinien zostać wypromowany jako serwer podstawowy bez przerwy w działaniu usług.

Usługi wspomagające

Kontroler domeny

Należy uruchomić min. dwa kontrolery domeny w trybie zalecanym przez producenta systemu domeny.

Serwer plików

Należy uruchomić serwer plików.

DNS

Należy uruchomić min. dwa serwery DNS..

NTP

Należy uruchomić min. dwa serwery NTP.

Zakres 3 – Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym sprzętem

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu administrowania zainstalowanymi Systemami na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia.

Szkolenia są niezbędne w celu zagwarantowania osiągnięcia zakładanych efektów w projekcie.

Szczegółowy zakres poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiającym.

Wykonawca na etapie uzgadniania materiałów szkoleniowych przekaże minimalne wymagania, jakie powinni spełniać oddelegowani przez Zamawiającego, uczestnicy szkolenia.

Do każdego modułu wspomagającego obsługę obszarów działalności, Zamawiający wskaże osoby, które Wykonawca przeszkoli.

Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych – dopuszcza prowadzenie szkoleń e-learningowych jedynie w ramach szkoleń uzupełniających.

Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 20 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych – dot. szkoleń certyfikowanych wyjazdowych.

W przypadku konieczności zorganizowania szkolenia poza siedzibą Zamawiającego – np. szkolenia certyfikowane producenta – Wykonawca pokryje koszty przejazdu, zakwaterowania i wyżywienia osób skierowanych na szkolenia.

Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiającego w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.

Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu. Szkolenie musi obejmować co najmniej instalację, konfigurację, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.

Uzgodnieniu pomiędzy stornami podlegają:

- Poziom szkoleń w zależności od wiedzy i umiejętności osób skierowanych na szkolenia,
- Harmonogram szkoleń,
- Materiały szkoleniowe dla szkoleń grupowych,
- Listy obecności ze szkoleń grupowych i indywidualnych,
- Protokoły odbioru zadania dot. szkoleń.

Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać

pracownikom na rozpoczęcie pracy w systemie.

Zakres 4 - Wdrożenie Systemu EOD

Wykonawca przeprowadzi prace wdrożeniowe w podziale na trzy etapy:

- Analiza przedwdrożeniowa,
- Instalacja, dostawa licencji Oprogramowania oraz Oprogramowania Narzędziowego, Konfiguracja oraz parametryzacja Systemu
- Szkolenia,

I etap: Analiza przedwdrożeniowa - będzie obejmować:

- Analizę infrastruktury technicznej biura obsługi interesanta w zakresie niezbędnego do obsługi EOD sprzętu,
- Przygotowanie przez Wykonawcę opisu danych konfiguracyjnych, które powinny zostać przygotowane przez Zamawiającego (np. dane adresowe, NIP itp.),
- Przesłanie do Zamawiającego arkuszy konfiguracyjnych w celu pozyskania danych wraz z instrukcją wypełniania arkuszy,
- Weryfikację opisanych w studium wykonalności lub opracowanie przez Wykonawcę definicji procesów (procedur WorkFlow) wspomaganych przez System Elektronicznego Obiegu Dokumentów.
- Przygotowanie oraz przedstawienie do akceptacji Zamawiającego szczegółowego harmonogramu szkoleń oraz wdrożenia Systemu Elektronicznego Obiegu Dokumentów
- Wykonawca zobowiązany jest do zaproponowania scenariuszy testowych wdrażanego Systemu. Zaakceptowane przez Zamawiającego scenariusze będą podstawą do przeprowadzenia odbiorów.

Zamawiający przekaże dane konfiguracyjne w przygotowanych przez Wykonawcę arkuszach konfiguracyjnych w terminie do 20 dni od daty ich otrzymania od Wykonawcy.

II etap: Instalacja, dostawa licencji Oprogramowania oraz Oprogramowania Narzędziowego, Konfiguracja oraz parametryzacja Systemu - będzie obejmować:

- Dostawę i instalację niezbędnego do obsługi EOD sprzętu (skanery, drukarki, itp.), Oprogramowania EOD oraz Oprogramowania Narzędziowego na serwerach wskazanych przez Zamawiającego, w tym:
  - Dostarczyć licencje, zainstalować i skonfigurować serwer SQL (serwer wyposażony będzie w 6 rdzeni),
  - Zainstalować i skonfigurować serwer aplikacji (np. IIS, apache2, tomcat, itp.),
  - Zainstalować i skonfigurować system EOD.

- Wprowadzenie procesów (procedur WorkFlow) obsługiwanych przez System EOD
- Wprowadzenie danych konfiguracyjnych dla EOD
- Wprowadzenie danych konfiguracyjnych dla Użytkowników Końcowych
- Wprowadzenie danych konfiguracyjnych niezbędnych do połączenia Systemu Elektronicznego Obiegu Dokumentów z innymi systemami (w tym ePuap i SD)
- Wprowadzenie i publikacja formularzy elektronicznych wdrażanych procedur administracyjnych
- Wykonawca zobowiązany jest do przeprowadzenia testów akceptacyjnych w siedzibie Zamawiającego. W testach musi uczestniczyć pracownik Wykonawcy oraz przedstawiciel Zamawiającego.

Wymagania minimalne dot. EOD

Zakup będzie obejmował dostawę licencji systemu elektronicznego obiegu dokumentów. System umożliwi przekazywanie i obsługę korespondencji w formie elektronicznej w ramach Urzędu Gminy. System musi być zintegrowanym pakietem oprogramowania do zarządzania dokumentami papierowymi i w postaci plików XML, korespondencją, sprawami oraz poleceniami oparty o Rzeczowy Wykaz Akt (RWA) lub podobną metodę klasyfikacji, oraz instrukcję obiegu dokumentów elektronicznych wraz z wykorzystaniem podpisu elektronicznego. Całość powinna być zbudowana i działać zgodnie ze światowymi standardami i wymogami prawa, w tym - z ustawy o informatyzacji podmiotów realizujących zadania publiczne, ustawy o podpisie elektronicznym oraz innymi przepisami powstałymi z delegacji tych ustaw.

Architektura systemu musi być otwarta i oparta na działających niezależnie od innych usługach, które

będą posiadać wyspecyfikowane interfejsy. Aplikacja powinna również umożliwiać integrację

z modernizowanymi w projekcie programami dziedzinowymi, a także krajową platformą e-PUAP.

System musi być zgodny z aktami prawnymi regulującymi pracę urzędów oraz realizacji e-usług.

System funkcjonalnie będzie pozwalać na tworzenie centralnej, uporządkowanej bazy dokumentów

i informacji, pism przychodzących i wychodzących, poleceń służbowych, umów, uchwał, regulacji

wewnętrznych itp. Będzie również organizować i systematyzować występujące w różnych formatach

dokumenty, usprawniać dostęp do informacji, kontrolować drogę ich obiegu, stan realizacji oraz

usprawnić obsługę klientów i obywateli.

Minimalne wymagania systemu elektronicznego obiegu dokumentów

Wymagania zgodności z obowiązującymi przepisami:

1. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 1960 r. Nr 30 poz. 168 z późn. zm.).
2. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. 1983 r. Nr 38 poz. 173 z późn. zm.).
3. 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. 2002 r. Nr 167 poz. 1375).

4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie nie-zbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006 r. Nr 206 poz. 1517).

5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. 2006 r. Nr 206 poz. 1518).

6. 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. 2006 r. Nr 206 poz. 1519).

7. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 r. Nr 133 poz. 883).

8. 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. 2004 r. Nr 100 poz. 1024).

9. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2001 r. Nr 112 poz. 1198).

10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 r. Nr 10 poz. 68).

11. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2001 r. Nr 130 poz. 1450).

12. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 r. Nr 144 poz. 1204).

13. Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. 2005 r. Nr 64 poz. 565) wraz z obowiązującymi aktami wykonawczymi.

14. Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. 2005 r. Nr 205 poz. 1692).

15. 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. 2005 r. Nr 217 poz. 1836).

16. Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną s dostępie warunkowym (Dz. U. 2002 r. Nr 126 poz. 1068 z późn. zm.).

17. Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. 2010 nr 40 poz. 230).

18. Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. z dnia 2 marca 2004 r.).

Wymagania architektury i technologii:

1. System powinien być zbudowany w architekturze trójwarstwowej, złożonej z:

a. programu klienckiego (kod generowany dla przeglądarki internetowej),

b. serwera aplikacji (kod zarządzający aplikacją, wykonujący funkcje z zakresu logiki biznesowej, pośredniczący między żądaniami programu klienckiego, a funkcjami udostępnianymi przez motor bazy danych),

c. motoru bazy danych, zarządzającego relacyjną i transakcyjną bazą danych SQL.

2. System powinien umożliwiać pracę na minimum jednej bazie komercyjnej oraz jednej bazie typu Open Source.

3. Zastosowany motor bazy danych powinien umożliwiać, a warstwa aplikacyjna systemu wykorzystywać podzapytania (ang. subqueries), kontrolę spójności referencyjnej danych (ang. referential integrity), wbudowane języki proceduralne (ang. stored procedural languages), rozbudowane indeksy, klucze obce, sekwencje, kursory, widoki, definiowane typy.

4. System powinien spełniać wszystkie funkcje wymagane do wdrożenia EOD zgodnie z rozporządzeniem Prezesa Rady ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011, Nr14, poz. 67).

5. W warstwie bazodanowej system powinien gwarantować dokonywanie operacji w oparciu o mechanizmy transakcji.

6. System w warstwie klienckiej musi poprawnie działać z co najmniej następującymi przeglądarkami WWW z obsługą Wirtualnej Maszyny Javy:

a. Microsoft Internet Explorer lub Edge,

b. Mozilla Firefox od wersji 30,

c. Google Chrome od wersji 35,

Interfejs użytkownika i administratora systemu powinien być obsługiwany co najmniej przez powyższe przeglądarki WWW.

7. Z uwagi na wycofanie wsparcia Oracle dla obsługi apletów JAVA niedopuszczalne jest wykorzystywanie w systemie apletów JAVA np. do obsługi skanera, faksu, składania i weryfikacji podpisu elektronicznego oraz funkcji administracyjnych.

8. Dostarczony system powinien posiadać polskojęzyczny interfejs użytkownika oraz obsługę polskich liter i sortowania wg polskiego alfabetu. Dotyczy to całego obszaru systemu.

9. Interfejs użytkownika systemu udostępniany przez przeglądarkę internetową powinien wykorzystywać techno-logię AJAX lub inne równoważne rozwiązanie, w celu przyspieszenia pracy.

10. Dopuszczalne formaty przetwarzanych plików nie mogą być ograniczone przez technologię systemu.

11. Do wymiany danych system wykorzystuje format XML.

12. System powinien być skalowalny, przy czym skalowanie może odbywać się przez:

a. dołączanie dodatkowych użytkowników do obsługi systemu,

b. zwiększenie zasobów komputerów obsługujących warstwę aplikacyjną poprzez rozbudowę pamięci, zwiększenie liczby procesorów,

c. zwiększenie zasobów komputerów obsługujących warstwę bazy danych poprzez rozbudowę pamięci, zwiększenie liczby procesorów, zwiększenie pojemności pamięci masowych).

14. Wszystkie dostarczane komponenty oprogramowania w ramach systemu powinny tworzyć jednolity system informatyczny, w szczególności poprzez wykorzystanie wspólnej platformy systemowej serwerów aplikacji i baz danych, wykorzystanie jednej wspólnej bazy danych, wykorzystanie wspólnego interfejsu użytkownika, wykorzystanie wspólnych kartotek, słowników i rejestrów, wykorzystanie wspólnego i spójnego systemu uprawnień, jedno miejsce logowania się do poszczególnych modułów systemu.

15. System powinien pozwalać na jednoczesny dostęp do danych wielu użytkownikom oraz zapewnia ochronę tych danych przed utratą spójności lub zniszczeniem.

16. Komunikacja użytkownika z systemem powinna odbywać się za pomocą połączenia szyfrowanego SSL.

17. Wszelkie dokumenty (pliki) tworzone i przetwarzane przez system powinny ze względów bezpieczeństwa umożliwiać przechowywanie ich w bazie (repozytorium) odrębnej w stosunku do bazy przechowującej rdzenne dane dla systemu (możliwe jest skonfigurowanie kilku serwerów przechowujących repozytorium plików).

18. Poszczególne komponenty systemu powinny komunikować się ze sobą oraz z systemami zewnętrznymi w sposób zapewniający poufność danych. Rozwiązanie musi mieć możliwość pracy z wykorzystaniem protokołu SSL oraz VPN, w szczególności wymaganie dotyczy pracy użytkowników systemu z sieci zewnętrznej.

19. Uwierzytelnienie użytkowników w ramach systemu powinno odbywać się, co najmniej: za pomocą loginu i hasła, karty/tokenu lub innego nośnika zawierającego certyfikat kwalifikowany lub niekwalifikowany oraz za po-mocą protokołu LDAP lub równoważnego.

20. System powinien umożliwiać wygenerowanie nowego hasła dla istniejącego użytkownika (w przypadku, gdy zostanie ono utracone), z zachowaniem procedury bezpieczeństwa wymuszającej zmianę tymczasowego hasła przy pierwszym logowaniu.

21. System powinien posiadać mechanizm bezpieczeństwa polegający na automatycznym generowaniu i weryfikacji sum kontrolnych dla każdego z plików dołączonych w aplikacji przez użytkownika i umożliwiają aplikacji automatyczne potwierdzenie jego wiarygodności. System powinien na bieżąco informować w trakcie przeglądania dokumentów o naruszeniach integralności plików sprawdzając sumę kontrolną.

22. Poszczególne elementy systemu powinny się dwukierunkowo kontaktować w oparciu o protokół SOAP (Simple Object Application Protocol). Wykonawca musi zapewnić bezpieczne mechanizmy komunikacyjne umożliwiające autoryzację zapytań i identyfikacje odpowiedzi.

23. System powinien pracować w środowisku sieciowym.

24. System powinien uniemożliwiać wprowadzanie i modyfikację danych w sposób anonimowy.

25. System powinien być odporna na zawieszanie się stacji roboczych, tj. usterka stacji roboczej w trakcie pracy w systemie nie może spowodować niestabilności pracy systemu dla pozostałych użytkowników.

26. System powinien umożliwiać określenie czasu nieaktywności, po którym wyloguje użytkownika.

Wymagania administracyjne:

1. System powinien umożliwiać zdefiniowanie wielopoziomowej struktury organizacyjnej, składającej się, co naj-mniej z jednostek organizacyjnych, komórek organizacyjnych, zespołów oraz stanowisk w dowolnej liczbie. Administrator w systemie może zmieniać strukturę organizacyjną w zależności od potrzeb i typu danej jednostki.

2. System powinien umożliwiać tworzenie zespołów zadaniowych, których członkami są dowolnie wybrani użytkownicy systemu, istniejących poza regularną strukturą urzędu. Niedopuszczalnym jest tworzenie dodatkowych identyfikatorów dla użytkowników przydzielonych do dodatkowych stanowisk (w tym do zespołów zadaniowych) lub zastępujących innych użytkowników.

3. System powinien umożliwiać przypisywanie użytkowników do stanowisk w strukturze organizacyjnej. Jeden użytkownik może być przypisany do kilku stanowisk z zachowaniem tego samego loginu i hasła dostępu do systemu.

4. System powinien umożliwiać definiowanie grup uprawnień użytkowników oraz dostępnych im funkcjonalności. System uprawnień musi umożliwiać odzwierciedlenie uprawnień i odpowiedzialności poszczególnych urzędników, stosowany w jednostkach samorządu terytorialnego i wynikający z Instrukcji Kancelaryjnych. Uprawnienia użytkowników są niezależne od systemu uprawnień systemu plikowego obsługiwanego przez system operacyjny lub motoru bazy danych i muszą w całości być obsługiwane przez aplikację.

5. System powinien umożliwiać określanie uprawnień widoczności dla użytkowników. Określanie takie polega na wskazaniu czyje dokumenty (i jakiego typu) widzi dany użytkownik.

6. System powinien umożliwiać przypisywanie zdefiniowanych grup uprawnień do stanowisk w strukturze organizacyjnej.

7. System powinien posiadać mechanizmy pozwalające na dodanie nowego użytkownika do istniejącego stanowiska (wakat) bez konieczności ponownego nadawania uprawnień dla stanowiska. System powinien pamiętać grupy uprawnień przypisane do konkretnego stanowiska nawet w przypadku odłączenia użytkownika od stanowiska w strukturze organizacyjnej w systemie.

8. System powinien umożliwiać modyfikowanie struktury organizacyjnej przez uprawnionego użytkownika w taki sposób aby zachowana była historia zmian.

9. System powinien umożliwiać definiowanie przez administratora dowolnych typów dokumentów (np. list polecony, faktura, wniosek, zaproszenie, pismo), oraz powiązanie typów dokumentów z metadanymi opisującymi te dokumenty.

10. System powinien umożliwiać dowolne definiowanie metadanych dla obiektów w tym, co najmniej: przesyłek, dokumentów, akt spraw, umożliwiających wyszukiwanie i zarządzanie ww. obiektami.

11. System powinien umożliwiać autouzupełnianie metadanych z zarejestrowanej przesyłki, dokumentu, sprawy. Z poziomu aplikacji musi być możliwość podglądu wszystkich metadanych w formie raportu dla przesyłki, sprawy, itp.

12. System powinien zawierać mechanizm dziennika systemowego (dostępnego z poziomu interfejsu systemu), umożliwiającego zapisywanie oraz przeglądanie historii zmian obiektów i danych z określeniem, co najmniej: czasu i opisu zmian, informacji o użytkownikach, którzy tych zmian dokonali, elementów, których dotyczy zmiana oraz czynności, która spowodowała zmianę. System powinien umożliwiać filtrowanie zapisów dziennika systemowego oraz eksport dziennika systemowego do pliku w formacie, co najmniej: PDF, TXT, DOC, XLS, XML, HTML oraz CSV.

13. System powinien umożliwiać testowanie wydajności z poziomu interfejsu systemu na podstawie stworzonych przez Wykonawcę skryptów.

14. Moduł procesów pracy (workflow) powinien umożliwiać:

a. stworzenie dedykowanego procesu obsługi konkretnego typu obiektu w notacji BPMN,

b. automatyczną weryfikację poprawności i kompletności zaprojektowanego procesu,

c. przypisanie krokom procesowym akcji systemowych wykonywanych zarówno przez użytkowników jak i automatycznie przez system,

d. obsługę co najmniej następujących akcji systemowych na krokach procesu:

- wyświetlenie formularza,
- łączenie obiektów,
- wystawianie komunikatów,
- wysyłanie komunikatów na adres email,
- wysyłanie komunikatów SMS na numer telefonu,
- zmiana statusów dokumentu,
- automatyczna zmiana właściciela dokumentu,
- ręczna zmiana właściciela dokumentu (przekazanie dokumentu),
- automatyczne tworzenie obiektów,
- usuwanie dokumentów,
- aktualizacja danych w dokumencie,

e. realizację ścieżek alternatywnych w zdefiniowanych dedykowanych procesach,

f. redefinicję wdrożonych procesów, możliwość zapisu ścieżek procesów do centralnej bazy lub plików lokalnych, z zachowaniem historii (procesy już rozpoczęte),

g. przydzielanie praw dostępu do akcji procesowych na dokumencie co najmniej dla następujących ról:

• właściciel dokumentu,

• każdy kto ma dostęp do dokumentu,

• na podstawie zdefiniowanego uprawnienia,

h. definiowanie typów obiektów/dokumentów z możliwością określania zakresu atrybutów, domyślnych statusów oraz maski numeru,

i. tworzenie formularzy służących do wprowadzania dokumentów, na podstawie wcześniej zdefiniowanych typów obiektów/dokumentów,

j. umieszczanie na formularzach słowników tworzonych przez administratorów systemu,

k. definiowanie rejestrów z określaniem co najmniej:

• rodzajów dokumentów w nich wyświetlanych,

• atrybutów wyświetlanych w rejestrze,

• zakresu atrybutów po których istnieje możliwość filtrowania danych w rejestrze.

15. System powinien posiadać wbudowany dedykowany słownik JRWA. System powinien umożliwiać edycję JRWA z poziomu panelu administratora. JRWA ma posiadać możliwość edycji, rozbudowy o kolejne stopnie, ich opis oraz określenie kategorii archiwalnej oraz sposobu prowadzenia dokumentacji w konkretnej klasie JRWA.

16. Administrator powinien mieć możliwość określenia daty od której obowiązywała będzie w systemie nowa wersja słownika JRWA.

17. System powinien umożliwiać zarządzanie słownikami z możliwością dodawania, usuwania, modyfikowania samych słowników lub pozycji słowników przez uprawione osoby. Aplikacja nie może pozwalać na usunięcie pozycji słownika lub samego słownika jeśli jest używany w systemie.

18. System powinien umożliwiać administratorowi ustalanie reguł złożoności hasła dla wszystkich użytkowników oraz określania, po jakim czasie użytkownik zostanie automatycznie zmuszony do zmiany hasła.

19. System powinien wyświetlać informacje dotyczące ilości i listę aktualnie zalogowanych użytkowników z możliwością wylogowania konkretnego użytkownika oraz globalnego zablokowania możliwości logowania do systemu.

20. System powinien umożliwiać definiowanie zastępstw przez użytkowników z określonymi uprawnieniami. Określając zastępstwo należy wskazać stanowisko zastępowane, stanowisko zastępujące oraz zakres dat w których obowiązywać będzie zastępstwo.

21. System powinien umożliwiać dostęp do konta pracownika zastępowanego przez pracownika zastępującego bez konieczności podawania hasła dostępu pracownika zastępowanego. Wszystkie czynności wykonane w zastępstwie powinny zawierać informację przez kogo faktycznie zostały wykonane.

22. System oprócz mechanizmu zastępstw powinien umożliwiać tzw. "pracę w imieniu". Definiując pracę w imieniu, oprócz wskazania stanowiska zastępowanego, stanowiska zastępującego oraz zakresu dat w których obowiązywać będzie "praca w imieniu" należy jeszcze określić do jakich czynności i jakich dokumentów dostęp będzie mieć użytkownik pracujący w imieniu innego użytkownika.

23. System powinien umożliwiać dostęp do konta pracownika zastępowanego w ramach "pracy w imieniu" przez pracownika zastępującego bez konieczności podawania hasła dostępu pracownika zastępowanego. Wszystkie czynności wykonane w ramach "pracy w imieniu" powinny zawierać informację przez kogo faktycznie zostały wykonane.

Przesyłki wpływające:

1. System powinien umożliwiać przyjmowanie korespondencji:

a. przychodzącą pocztą elektroniczną na dowolny adres e-mail urzędu, komórki organizacyjnej, bądź pracownika,

b. złożonej w postaci plików elektronicznych na nośnikach cyfrowych (system teleinformatyczny umożliwia wystawienie UPO w wersji elektronicznej lub przygotowanie potwierdzenia do wydruki wersji papierowej),

c. z Elektronicznej Skrzynki Podawczej (ESP) udostępnianej:

• przez ePUAP,

• przez inny podmiot podłączony przez interfejs sieciowych wg udokumentowanej specyfikacji technicznej przez Wykonawcę (zadaniem Wykonawcy jest przygotowanie interfejsu sieciowego i opracowanie dokumentacji technicznej podłączenia ESP).

2. System powinien umożliwiać rejestrację papierowej korespondencji przychodzącej i przetwarzanie do postaci wtórnych dokumentów elektronicznych (odwzorowań cyfrowych). Rejestracja tych przesyłek polega na odwzorowaniu cyfrowym przesyłki, dołączeniu go do zarejestrowanej korespondencji oraz ma możliwość dołączania odpowiednich metadanych brakujących w systemie.

3. Moduł do skanowania dokumentów powinien umożliwiać minimum:

a. skanowanie czarno-białe lub w kolorze oraz redukcję kolorów do odcieni szarości i czarno-białego,

b. skanowanie we wszystkich rozdzielczościach udostępnianych przez wykorzystywany sprzęt (skanery),

c. skanowanie z wykorzystaniem profili skanowania zgodnych z Instrukcją Kancelaryjną oraz definiowanie nowych profili skanowania przez administratora,

d. usuwanie dowolnej strony w zeskanowanym wielostronicowym dokumencie,

e. dodawanie nowych stron skanu dokumentu pomiędzy istniejące strony skanu,

f. możliwość dołączania plików (z dysku) do listy wcześniej zeskanowanych stron dokumentu

g. obracanie skanów w lewo, w prawo i o 180 stopni oraz obracanie obrazu o dowolną liczbę stopni,

h. wykrywanie i usuwanie pochylenia tekstu,

i. przycinanie i kadrowanie zeskanowanego dokumentu,

j. skalowanie zeskanowanego dokumentu,

k. odwracanie kolorów (negatyw) w zeskanowanym dokumencie.

4. System powinien umożliwiać sporządzenie potwierdzenia zawierającego unikalny identyfikator przesyłki prezentowany w postaci znakowej i kodu kreskowego (w formie nadruku lub naklejki). Identyfikator przesyłki może być umieszczany również na dowolnym dokumencie związanym z niniejszą przesyłką lub sprawą. Na wygenerowanym potwierdzeniu powinny znaleźć się m.in.: data wpływu, liczba załączników, dane podmiotu/osoby składającej pismo, dane użytkownika, który pismo zarejestrował.

5. System powinien posiadać tryb szybkiej rejestracji przychodzących pism. Przez szybką rejestrację należy rozumieć rejestrację ograniczoną tylko do nadania kolejnego identyfikatora dokumentu,

numeru wpływu, określenia daty, a także wygenerowanie potwierdzenia zawierającej informacje o złożonym dokumencie.

6. W dowolnym momencie System powinien umożliwiać dokończenie pełnej rejestracji korespondencji zarejestrowanej w trybie szybkiej rejestracji.

7. System powinien umożliwiać skanowanie wielu dokumentów opatrzonych kodami kreskowymi z automatycznym rozdzieleniem ich na poszczególne pliki na podstawie kodów kreskowych.

8. System powinien umożliwiać automatyczne rozpoznanie kodu kreskowego i automatyczne dołączanie na jego podstawie skanu do metadanych w systemie.

9. System powinien umożliwiać określenie rodzaju pisma za pomocą pola słownikowego.

10. Zarejestrowane pisma przychodzące mają tworzyć automatycznie dziennik korespondencji przychodzącej.

11. System powinien umożliwiać tworzenie dodatkowych dzienników/rejestrów dla wydziałów, komórek organizacyjnych.

12. System powinien umożliwiać umieszczenie dodatkowych metadanych tj. innych niż wymaganych w Instrukcji Kancelaryjnej dla korespondencji przychodzących.

13. System powinien posiadać mechanizm umożliwiający sprawdzenie podczas rejestracji czy przychodząca korespondencja nie została już wprowadzona do systemu np. w postaci innego dokumentu - sprawdzenie np. po nr pisma nadawcy.

14. System powinien umożliwiać rejestrację przesyłek przekazanych na informatycznym nośniku danych. Rejestracji podlega dokument elektroniczny. System powinien umożliwiać dodanie załączników lub informacji o nie dołączonych załącznikach (np. dużych dokumentach, innych nie możliwych do dołączenia) oraz generuje automatycznie Urzędowe Poświadczenie Odbioru (UPO). System umożliwia zarejestrowanie numeru seryjnego nośnika.

15. System powinien umożliwiać przyporządkowywanie przesyłkom wpływającym minimum zakresu metadanych zgodnie z Instrukcją Kancelaryjną.

16. System powinien automatycznie nadawać przesyłce wpływającej identyfikator unikalny w zbiorze przesyłek wpływających (tzw. nr z rejestru).

17. System powinien umożliwiać uzupełnianie brakujących metadanych (nie wprowadzone podczas rejestracji), które mogą być uzupełniane w dowolnym momencie. System sygnalizuje brak obowiązkowych metadanych.

18. System powinien umożliwiać odnotowanie informacji w metadanych opisujących przesyłkę (w odniesieniu do każdej przesyłki z osobna), o nie dołączeniu pełnego odwzorowania cyfrowego i/lub plików przekazanych na nośniku informatycznym. Adnotacja musi zawierać wskazanie konkretnego nośnika (informatycznego i/lub papierowego), oraz miejsca jego przechowania (np. rejestr nośników informatycznych).

19. System powinien umożliwiać wyszukanie i sporządzenie listy przesyłek na informatycznych nośnikach danych, których nie włączono do systemu EOD, zawierającej w szczególności wskazanie nośników, na których się one aktualnie znajdują i wskazanie ich lokalizacji (tj. identyfikator nośnika w składzie nośników informatycznych, lokalizacja nośnika).

20. System powinien umożliwiać użytkownikom w kancelarii przekazywanie przesyłek wpisanych do rejestru przesyłek wpływających do komórek organizacyjnych i/lub stanowisk. Przekazywanie może się obywać ręcznie (”ad hoc”), lub automatycznie (zgodnie ze zdefiniowanym dedykowanym procesem.

21. System powinien dodawać automatycznie metadane do Dokumentów Elektronicznych zgodnie z Rozporządzeniem 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.

22. System powinien umożliwiać szybką rejestrację przesyłek od jednego nadawcy, pozwalając tworzyć kolejne dokumenty na podstawie wcześniej zarejestrowanego. Przy wykorzystaniu tego mechanizmu system uzupełnia metadane pobierając je z wcześniej zarejestrowanej przesyłki.

23. System powinien umożliwiać tworzenie zbiorów dokumentów podręcznych dla każdego użytkownika oddziel-nie. Dokumenty podręczne powinny być umieszczane w strukturze katalogowej budowanej przez użytkownika i pamiętanej przez system. Dokumenty podręczne powinny zapewniać szybki dostęp do dokumentów i przesyłek bez konieczności przeglądania rejestrów w których przesyłki/dokumenty się znajdują.

24. System powinien umożliwiać na definiowanie i korzystanie z grup w momencie dekretacji. Dekretacja na zdefiniowaną grupę powoduje przekazanie pisma do wiadomości do wszystkich komórek/stanowisk znajdujących się w zdefiniowanej grupie do dekretacji.

25. System powinien umożliwiać określenie czy zdefiniowana grupa do dekretacji jest grupą publiczną (dostępną dla każdego użytkownika) czy prywatną (dostępną tylko dla użytkownika, który ją stworzył).

26. System powinien umożliwiać wielopoziomową dekretację w zależności od nadanych uprawnień.

27. Podczas dekretacji powinno być możliwe przekazywanie pisma dowolnej liczbie pracowników i/lub komórek organizacyjnych zgodnie ze strukturą organizacyjną.

28. System powinien umożliwiać kierowanie przesyłek do osoby z wykorzystaniem kryterium najmniejszego obciążenia stanowiska (najmniejsza liczba procedowanych przez niego w danym momencie spraw).

29. System powinien umożliwiać masową dekretację, tj. dekretację co najmniej dwóch pism jednocześnie z zaznaczeniem komórki/stanowiska wiodącej/wiodącego i do wiadomości.

30. System powinien umożliwiać dekretację i przesyłanie przesyłki jednocześnie do wielu komórek organizacyjnych wykorzystując do tego celu słowniki: struktury organizacyjnej, użytkowników oraz stanowisk.

31. System powinien umożliwiać uprawnionym użytkownikom wykonywanie dekretacji. W szczególności proces dekretacji umożliwia dekretującemu wskazanie:

a. stanowiska lub komórki organizacyjnej wyznaczonej do załatwienia sprawy,

b. terminu załatwienia sprawy i/lub pisma,

c. sposobu załatwienia sprawy i/lub pisma, oraz opatrzenie dekretacji odpowiednim podpisem elektronicznymi.

Każde polecenie dekretacyjne powinno być dołączone do przesyłki tworząc historię poleceń dekretacyjnych.

32. System powinien umożliwiać wielokrotną dekretację wykonywaną przez uprawnionych użytkowników, z tym zastrzeżeniem, że nie może ona powodować utraty treści poprzednich dekretacji oraz musi umożliwiać zmianę terminu załatwienia sprawy wskazanego w pierwotnej dekretacji.

33. System powinien umożliwiać użytkownikom zwrócenie zadekretowanej przesyłki do użytkownika będącego au-torem dekretacji, także w przypadku dekretacji wielostopniowych.

34. System powinien posiadać podgląd pisma przewodniego lub załączników co najmniej będącego w formacie PDF, DOC, TXT, TIFF.

35. System powinien umożliwiać dołączanie przesyłek do teczek dokumentów nietworzących akta sprawy. Numeracja teczki dokumentów nietworzących akta sprawy powinna zawierać: symbol komórki organizacyjnej w której powstała, symbol teczki JRWA oraz rok (czterocyfrowy).

36. System powinien umożliwiać oznaczenie pisma wpływającego jako "prywatne". Tak oznaczone pismo powinno być widoczne tylko dla użytkownika, który w taki sposób oznaczył przesyłkę.

Przesyłki wychodzące:

1. System powinien wspomagać obsługę przesyłek wychodzących poprzez automatyczne prowadzenie rejestru pism wychodzących.

2. Na rejestr przesyłek wychodzących powinny składać się przesyłki wysyłane przez referentów z poziomu spraw jak i te wysyłanie z pominięciem rejestrowania ich w aktach sprawy (np. zaproszenia).

3. Rejestr przesyłek wychodzących umożliwia wygenerowania pocztowej książki nadawczej dla określonych dat, typów przesyłek (zgodnie z wybranymi przez użytkownika kryteriami), a także drukowanie kopert, pocztowych potwierdzeń odbioru (tzw. zwrotek) oraz naklejek adresowych.

4. System powinien umożliwiać łączenie wielu pism do jednej koperty, co skutkuje jednym wpisem do pocztowej książki nadawczej dla tych kilku pism.

5. Wzór pocztowej książki nadawczej powinien być zgodny z regulacjami Poczty Polskiej.

6. System powinien umożliwiać obsługę przesyłek wychodzących obsługiwanych przez gońców poprzez:

a. przydzielanie przesyłek gońcom z uwzględnieniem rejonizacji przesyłek przeznaczonych do doręczenia w danym dniu,

b. umożliwiać generowania wydruków książki doręczeń,

c. wprowadzenie informacji o doręczeniu przesyłek dostarczonych przez gońców w dniu następnym,

d. jednoczesną obsługę wielu gońców.

7. System powinien umożliwiać szybkie wyszukanie przesyłek wychodzących przeznaczonych do wysyłki i oznaczenie ich jako „wychodzące" w danym dniu.

8. Rejestracja przesyłek wychodzących powinna uwzględniać opcjonalne określania kosztów wysyłki poprzez wykorzystanie słownika kosztów przesyłek.

9. System powinien umożliwiać rejestrację zwrotów przesyłek oraz pocztowych potwierdzeń odbioru (tzw. zwrotek) z poziomu rejestru przesyłek wychodzących (bezpośrednio przy przesyłce wychodzącej). Rejestracja zwrotu lub zwrotki ma skutkować zmianą statusu przesyłki wychodzącej oraz automatycznym pojawieniem się zarejestrowanego zwrotu/zwrotki w teczce sprawy przy właściwym dokumencie.

10. System powinien umożliwiać:

a. doręczanie przesyłek wychodzących na adres elektroniczny klienta (na platformie ePUAP),

b. obsługę i przechowanie w EOD poświadczenia doręczenia oraz poświadczenia przedłożenia, zgodnie z przepisami prawa tj., rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011r. w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych. (Dz.U. z 2011, Nr206, poz.1216).

11. System powinien umożliwiać przyporządkowywanie przesyłkom wychodzącym pełnego zakresu metadanych zgodnie z Instrukcją Kancelaryjną. System powinien umożliwiać przyporządkowanie dodatkowych metadanych nie ujętych w Instrukcji Kancelaryjnej.

12. System powinien umożliwiać użytkownikom w kancelarii potwierdzenie wysyłki przesyłek, wskazanie daty wysyłania, sposobu wysłania oraz uzupełnienie metadanych opisujących przesyłkę.

13. System powinien umożliwiać:

a. Zapisanie w rejestrze Klientów informacji o adresie poczty elektronicznej i/lub adresie skrytki Klienta na ePUAP,

b. w konfiguracji danych o Kliencie musi istnieć możliwość powiązania odpowiednich informacji przechowywanych w rejestrze oświadczeń o: wyrażeniu, cofnięciu, zmianie zgody/żądania na obsługę przesyłek/pism drogą elektroniczną,

c. Wybór adresu Klienta, który wyraził zgodę/żądanie na obsługę przesyłek/pism drogą elektroniczną, oznacza, że automatycznie zostanie określony sposób wysyłki przesyłki wskazany przez Klienta.

d. W przypadku, gdy nie ma możliwości wysyłki przesyłki/pisma drogą elektroniczną, przesyłka/pismo zostaje wysyłane w formie tradycyjnej (papierowej).

14. System do tworzenia pism wychodzących powinien wykorzystywać Wzory Dokumentów Elektronicznych gromadzone w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych na ePUAP.

15. System powinien umożliwiać przekazywanie dokumentu do akceptacji zgodnie ze zdefiniowaną uprzednio ścieżką akceptacji.

16. System powinien umożliwiać wersjonowanie dokumentów w przypadku tworzenia kolejnych wersji istniejących dokumentów oraz przywracanie starszych wersji dokumentów.

17. System powinien posiadać wbudowany edytor tekstowy dokumentów z wykorzystaniem wyłącznie przeglądarki internetowej bez konieczności załączania dokumentów tworzonych w zewnętrznych aplikacjach. Edytor treści pozwala na proste formatowanie tekstu w tym co najmniej: (boldowanie, kursywa, podkreślenie, zmiana rozmiaru czcionki, punktory, justowanie, wyśrodkowanie, wyrównanie do lewej, wyrównanie do prawej).

18. System powinien umożliwiać dołączanie załączników do pism w postaci plików w dowolnym formacie.

19. System powinien umożliwiać, zgodnie z uprawnieniami, modyfikację danych w metadanych dokumentu na do-wolnym etapie akceptacji. W takim wypadku, wymagane jest zachowywanie pełnej historii wszystkich wprowadzonych zmian w metryce z możliwością ich podejrzenia. Wprowadzenia zmian w dokumencie po jego akceptacji skutkuje automatycznym wymuszeniem ponowienia ścieżki akceptacji.

20. System powinien umożliwiać użytkownikom akceptację dokumentów, w szczególności poprzez podpisywanie dokumentu elektronicznego odpowiednim podpisem elektronicznym.

21. System powinien umożliwiać wielokrotne podpisywanie podpisem elektronicznym dokumentów elektronicznych.

22. System powinien domyślnie prezentować użytkownikom ostatnią wersję sporządzonego pisma/dokumentu i wraz z opisującymi je metadanymi, prezentacja ich wcześniejszych wersji odbywa się na żądanie użytkownika.

Praca ze sprawami:

1. System powinien umożliwiać wszczęcie sprawy z urzędu tzn. zainicjowanie sprawy przez referenta na stano-wisku pracy.

2. System powinien umożliwiać użytkownikom tworzenie spraw i oznaczanie ich znakiem sprawy zgodnym z for-matem ustalonym w obowiązującej Instrukcji Kancelaryjnej w pełnym zakresie możliwości oznaczeń.

3. System powinien gromadzić pełną dokumentację dotyczącą sprawy w postaci elektronicznej teczki sprawy, która zawiera całość akt postępowania włącznie z wersjami roboczymi dokumentów. System nie powinien ograniczać liczby Interesantów, dokumentów, przesyłek, które mogą być zarejestrowane w teczce sprawy.

4. System powinien umożliwiać prezentację i wydruk metryki sprawy zgodnej z KPA lub z Ordynacją Podatkową (w zależności od wyboru na etapie wszczynania sprawy).

5. Każda sprawa powinna móc zostać przez użytkownika komórki merytorycznej na dowolnym etapie wstrzymana bądź zawieszona oraz w każdym momencie kontynuowana. W takim wypadku, aplikacja wymusza określenie powodu dokonania takiej operacji w systemie.

6. System powinien umożliwiać przyporządkowywanie sprawom pełnego zakresu metadanych zgodnie z Instrukcją Kancelaryjną.

7. System powinien umożliwiać kontynuowanie spraw założonych w roku poprzednim, bez zmiany ich dotychczasowych znaków.

8. System powinien umożliwiać uprawnionemu użytkownikowi założenie nowej sprawy będącej kontynuacją innej sprawy. W takiej sytuacji aplikacja wiąże ze sobą obie sprawy odpowiednią relacją tak, aby w każdej ze spraw znajdowała się informacja co najmniej o powiązaniu oraz wskazanie znaku sprawy powiązanej.

9. System powinien umożliwiać wprowadzanie do spraw wszelkich dokumentów, projektów pism, notatek i adnotacji, zgodnie z uprawnieniami użytkownika.

10. System powinien umożliwiać uprawnionym użytkownikom komórek merytorycznych udostępnianie akt spraw innym użytkownikom (również innych komórek organizacyjnych niż merytoryczna) oraz określenie zakresu udostępnienia, w szczególności:

a. wskazanie dokumentacji stanowiącej akta sprawy,

b. wskazanie zakresu dostępu (odczyt, edycja dokumentów, umieszczanie nowych dokumentów).

11. System powinien umożliwiać wielu użytkownikom (również z różnych komórek organizacyjnych) pracę nad jedną sprawą, bez konieczności tworzenia wielu egzemplarzy dokumentacji.

12. System powinien umożliwiać użytkownikom akceptującym projekty pism i dokumentów nanoszenie do ww. projektów uwag oraz adnotacji. System powinien przechowywać wszystkie wersje akceptowanych pism w aktach sprawy.

13. System powinien umożliwiać użytkownikowi prowadzącemu sprawę wskazanie daty wysyłania i uzupełnienie metadanych opisujących przesyłkę w dowolnym momencie procedowania sprawy.

14. System powinien umożliwiać przyporządkowywanie elementom akt sprawy nie będących przesyłkami, zestawu pełnego zestawu metadanych zgodnie z Instrukcją Kancelaryjną.

15. System powinien umożliwiać użytkownikowi wybranie teczki JRWA ze słownika JRWA lub z podręcznie listy wcześniej użytych teczek przez danego użytkownika.

16. System powinien umożliwiać automatyczne przepisywanie metadanych pomiędzy dokumentami i sprawami np.: strony sprawy, data wszczęcia itd…

17. System powinien umożliwiać bieżące monitorowanie i informowanie użytkownika o zbliżających się terminach.

18. System powinien oznaczać w specjalny sposób, co najmniej sprawy przeterminowane oraz bliskie przeterminowaniu.

19. System powinien umożliwiać przełożonym pełny wgląd w sprawy prowadzone przez podwładnych.

20. W systemie powinna istnieć możliwość przejmowania spraw podwładnych i/lub ich przekazywania innym pracownikom.

21. W systemie powinna istnieć możliwość zmiany terminu zakończenia sprawy.

22. System powinien umożliwiać przełożonym i/lub uprawnionym użytkownikom kontrolę terminowości załatwiania spraw, zgodnie z uprawnieniami.

23. System powinien umożliwiać uprawnionym użytkownikom przegląd spisów spraw i zawartości teczek spraw komórek organizacyjnych.

24. System powinien umożliwiać uprawnionym użytkownikom przeglądanie statystyk dotyczących obiegu dokumentów i prowadzonych spraw we własnej komórce i komórkach podległych.

25. Uprawnieni użytkownicy powinni mieć prawo do przeglądania statystyk dotyczących wszystkich spraw, dokumentów całego urzędu.

Edytory dokumentów, szablony

1. System powinien umożliwiać stworzenie formularza elektronicznego do wprowadzania danych w systemie. Edytor formularzy w systemie:

a. Powinien posiadać graficzny interfejs użytkownika pracujący w trybie WYSWIG pozwalający na wykorzystanie następujących typów pól i elementów przy tworzeniu formularza:

• lista rozwijalna (ang. list box),
• obszar tekstowy (ang. text area),
• pole tekstowe (ang. text field),
• pole zaznaczenia (ang. checkbox),
• pole wyboru (ang. radio),
• blok powtarzalny,
• sekcja warunkowa (element na formularzu pojawiający się po spełnieniu zdefiniowanego warunku),
• link umożliwiający umieszczenie adresu URL,
• pole data (z możliwością wykorzystania kalendarza do wypełnienia danych),
• załączników,
• elementy ze struktury organizacyjnej,
• dane klienta z bazy klientów w aplikacji,
• słowniki zdefiniowane w systemie,
• zewnętrzne źródło danych (np. dane z bazy danych)

b. Powinien umożliwiać import/eksport formularzy elektronicznych do/z pliku XML/HTML,

c. Powinien umożliwiać walidację formularzy elektronicznych,

d. Powinien umożliwiać zdefiniowanie wymagalności podpisu elektronicznego na dokumencie stworzonym przy pomocy formularza.

2. System powinien umożliwiać eksport do pliku „*.PDF" wygenerowanego z formularza dokumentu.

3. System powinien posiadać wbudowany edytor WYSIWYG umożliwiający tworzenie dokumentów w oparciu o język XHTML.

4. System powinien posiadać wbudowany edytor szablonów dokumentów umożliwiający zaprojektowanie dowolnego szablonu dokumentu z użyciem danych dostępnych w systemie oraz metadanych dokumentu. Edytor szablonów dokumentów umożliwia wykorzystywanie w szablonach zmiennych związanych z danymi tekstowymi, liczbowymi, słownikowymi, wprowadzonymi na etapie rejestracji formularza dokumentu (wykorzystanie metadanych).

5. System powinien umożliwiać import szablonu stworzonego w formacie RTF. W szablonie musi istnieć możliwość automatycznego wstawiania wartości/danych dostępnych w systemie związanych z generowanym dokumentem. Zakres danych definiowany powinien być dla każdego typu obiektu/dokumentu oddzielnie.

6. System powinien umożliwiać umieszczanie szablonów w drzewiastej strukturze katalogów.

7. System powinien umożliwiać definiowanie uprawnień do stworzonych szablonów. Oddzielnie do edycji szablonu i oddzielnie do tworzenia dokumentów na podstawie szablonów.

8. System powinien umożliwiać definiowanie wydruków za pomocą edytora wbudowanego/uruchamianego z poziomu systemu. Definiowanie wydruków odbywać się powinno w oparciu o wszystkie dane dostępne w systemie.

Rejestry i spisy:

1. System powinien umożliwiać definiowanie i prowadzenie rejestrów (wydziałowych, urzędowych, innych) oraz wprowadzanie przesyłek, spraw i dokumentów do zdefiniowanych wcześniej rejestrów. System powinien umożliwiać generowanie raportów i zestawień ze zdefiniowanych rejestrów. Z chwilą zdefiniowania tych rejestrów, prowadzenie ich odbywa się w sposób automatyczny.

2. System powinien umożliwiać tworzenie rejestrów przesyłek przychodzących i wychodzących dla jednostki, oraz rejestry pomocnicze każdej komórki organizacyjnej.

3. Funkcjonalność rejestrów systemu powinna umożliwiać:

a. tworzenie wykazów spraw/ przesyłek/dokumentów w układach zawierających dowolnie wybrane dane do-tyczące spraw/przesyłek/dokumentów (w tym odpowiednie metadane spraw/przesyłek/dokumentów),

b. zdefiniowanie dowolnej liczby kolumn w rejestrze, które wypełniane będą automatycznie z danych dotyczących rejestrowanych spraw/przesyłek oraz takich, które będą uzupełniane „ręcznie" przez użytkownika, a także kojarzenie rejestrów z określonymi typami spraw/przesyłek i dokumentów.

4. System powinien pozwalać na automatyczne uzupełnianie danych w rejestrach (np. wpisy dokonywane po zatwierdzeniu dokumentu lub zarejestrowaniu sprawy).

5. System powinien umożliwiać dodanie wpisów do rejestru przez użytkownika, posiadającego odpowiednie uprawnienie.

6. System powinien posiadać wbudowane mechanizmy umożliwiające przesyłanie zawartości wskazanych rejestrów do publikacji w zewnętrznym systemie (np. BIP).

Archiwizacja spraw i dokumentów:

1. Czynności związane z obsługą archiwum powinny pozwalać na pełne udokumentowanie przeprowadzonych czynności. Wszelkie generowane spisy dokumentów oraz zawartość paczki archiwalnej powinny być zgodne z obowiązującym formatem wymiany danych udostępnionym przez Naczelną Dyrekcję Archiwów Państwowych.

2. System powinien umożliwiać tworzenie spisów zdawczo-odbiorczych, które stanowią podstawę do przyjmowania i przekazywania akt, teczek oraz innej dokumentacji w obrębie jednostki oraz wprowadzanie ręcznego spisu zdawczo-odbiorczego w przypadku przekazania dokumentów wraz ze spisem zdawczo-odbiorczym sporządzonym w systemie tradycyjnym.

3. System powinien umożliwiać wprowadzenie spisu dokumentów na nośnikach papierowych uprzednio przekazanych i będących już w Archiwum a nieewidencjonowanych w bazie danych systemu.

4. Po przyjęciu dokumentów do Archiwum, aplikacja automatycznie wylicza rok planowanego brakowania.

5. System powinien umożliwiać podgląd i wydruk zarejestrowanych spisów. W dowolnym momencie uprawniony użytkownik musi mieć możliwość podglądu oraz wydruku szczegółów poszczególnych pozycji w archiwum.

6. System powinien umożliwiać prowadzenie kompletnej ewidencji przechowywanej dokumentacji tak, aby istniała możliwość:

a. przeszukiwania zgromadzonej dokumentacji, według zadanych kryteriów,

b. sortowania materiałów archiwalnych wg typów symboli dokumentacji,

c. ewidencjonowania akt, które nie zostały zwrócone do archiwum, które zostały uszkodzone w trakcie wypożyczenia lub akt, których brakuje w wydziale, do którego uprzednio wypożyczono dane akta.

7. System powinien umożliwiać wydruk karty udostępnienia akt, dla dokumentacji przechowywanej w archiwum a nie ewidencjonowanej systemie.

8. System powinien generować identyfikatory kodów kreskowych (w formie nadruku lub naklejki) dla akt, teczek oraz innych dokumentów przekazywanych do archiwum. Funkcja ta ma ułatwić wyszukiwanie w bazie danych teczek oraz akt.

9. System powinien umożliwiać przeprowadzenie procesu brakowania akt oraz sporządzenie adnotacji o wykonaniu brakowania w odpowiedniej ewidencji. Proces ten będzie przeprowadzany przez użytkownika z odpowiednimi uprawnieniami, który musi mieć możliwość wyszukania akt, które będą poddane procesowi brakowania.

10. System powinien umożliwiać tworzenia spisów dokumentacji nie archiwalnej przeznaczonej na makulaturę lub zniszczenie, której okres przechowywania upłynął. Proces ten będzie przeprowadzany przez użytkownika z odpowiednimi uprawnieniami, który po przygotowaniu spisu będzie mógł go wydrukować.

11. System powinien umożliwiać przygotowanie dokumentacji archiwalnej w ramach komórki organizacyjnej do ekspertyzy w celu zatwierdzenia brakowania lub w celu zmiany kwalifikacji.

12. W dowolnym momencie uprawniony użytkownik modułu musi mieć możliwość odszukania sporządzonych spisów zdawczo-odbiorczych akt przekazanych do Archiwum Państwowego oraz na zniszczenie lub makulaturę.

13. System powinien pełnić rolę archiwum zakładowego dla dokumentacji gromadzonej i ewidencjonowanej.

14. System powinien umożliwiać uprawnionym użytkownikom na:

a. udostępnianie,

b. brakowanie,

c. przekazywanie do archiwum państwowego,

d. dodawanie adnotacji,

e. uzupełnianie meta danych dokumentacji przekazanej do archiwum zakładowego.

15. System powinien umożliwiać przekazanie uprawnień archiwiście do zarządzania dokumentacją w sposób automatyczny, po przekazaniu dokumentacji do archiwum.

16. System powinien umożliwiać uprawnionym użytkownikom wskazywanie dokumentacji, którą chcą przekazać do archiwum zakładowego.

17. System powinien umożliwiać generowanie spisów zdawczo-odbiorczych nośników informatycznych i papierowych przekazywanych do archiwum ze składów nośników.

18. System powinien umożliwiać udostępnienie dokumentacji z archiwum zakładowego, po uprzedniej akceptacji przez uprawnionego użytkownika.

19. System powinien umożliwiać ewidencjonowanie udostępnień i wypożyczeń dokumentacji z archiwum zakładowego, poprzez co najmniej wskazanie:

a. podmiotu, któremu dokumentację wypożyczono i/lub udostępniono,

b. udostępnionej i/lub wypożyczonej dokumentacji,

c. data wypożyczenia i zwrotu lub daty udostępnienia.

20. System powinien umożliwiać użytkownikowi archiwum wygenerowanie paczek archiwalnych dla dokumentacji przekazywanej do archiwum państwowego oraz sporządzenie adnotacji o przekazaniu dokumentacji w odpowiedniej ewidencji.

Wyszukiwarki:

1. System powinien umożliwiać wyszukiwanie dokumentów i spraw za pomocą wielu kryteriów, m.in. po metadanych opisujących dokumenty przetwarzane w systemie. Istnieje możliwość łączenia kryteriów w celu ograniczenia wyników wyszukiwania.

2. System powinien posiadać wyszukiwarkę globalną, której zakres wyszukiwania obejmuje całą bazę systemu, jak i kontekstowe wyszukiwarki dostępne i ograniczone do wyszukiwania w zakresie spraw/dokumentów danego modułu/zakresu (np. tylko rejestr poczty przychodzącej, tylko rejestr korespondencji wychodzącej itp.).

3. System powinien umożliwiać wyszukiwanie z użyciem symboli wieloznacznych.

4. System powinien umożliwiać pełnotekstowe wyszukiwanie dokumentów elektronicznych w repozytorium plików, co najmniej dla następujących formatów: TXT, PDF, DOC, RTF, XLS, PPT, ODT.

5. System powinien umożliwiać wyszukanie i sporządzenie listy przesyłek na nośnikach papierowych, których pełnych odwzorowań cyfrowych nie dołączono do metadanych je opisujących, zawierających, co najmniej wskazanie konkretnych nośników (tj. identyfikator nośnika w składzie chronologicznym nośników papierowych, lokalizacja nośnika).

6. System powinien mieć możliwość współpracy z czytnikami kodów kreskowych w celu wyszukiwania, lub od-czytania kodu maszynowego na identyfikatorze zamieszczonym na przesyłkach/elektronicznych nośnikach danych/sprawach/teczkach.

Podpis elektroniczny:

1. System powinien umożliwiać weryfikację podpisów elektronicznych, o których mowa w art. 20a ust. 1. ustawy z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne.

2. System powinien automatycznie wywoływać usługę weryfikacji podpisu elektronicznego w momencie pojawienia się w systemie dokumentu podpisanego takim podpisem.

3. System powinien umożliwiać ręczne wywołanie usługi weryfikacji podpisu elektronicznego z poziomu systemu w przypadku problemów z weryfikacją automatyczną np. brak dostępu do internetu w czasie automatycznego wywołania usługi weryfikacji.

4. System powinien umożliwiać podpisywanie dokumentów elektronicznych w formacie XAdES.

5. System powinien umożliwiać składanie wielu podpisów pod jednym dokumentem w formacie XAdES.

Raporty i statystyki:

1. System powinien umożliwiać monitorowanie przepływu pracy poprzez tworzenie raportów i statystyk.

2. System powinien posiadać gotowe raporty informujące o historii każdej sprawy:

a. wykaz wszystkich użytkowników pracujących nad daną sprawą, wraz z załączonymi przez nich dokumentami oraz wykonanymi czynnościami a także czasem przetwarzania przez nich sprawy w danym kroku procesu,

b. zestawienie liczby załatwionych spraw za dany okres, dla danego pracownika, grup pracowników, jedno-stek organizacyjnych, kategorii sprawy,

c. Ilości obsłużonych przesyłek za dany okres, dla danego pracownika, grup pracowników, jednostek organizacyjnych, kategorii przesyłek.

3. System powinien posiadać wbudowany generator raportów umożliwiający, co najmniej:

a. definiowanie typu raportu: dotyczący przesyłek lub spraw,

b. definiowanie zawartości kolumn raportów prezentowanych w postaci tabelarycznej na podstawie danych dostępnych w systemie,

c. definiowanie warunków po spełnieniu, którego informacja o danej sprawie bądź przesyłce znajduje się w raporcie np. pokaż sprawy przeterminowane w odpowiednim układzie.

4. System powinien:

a. umożliwiać tworzenie, edycję oraz usuwanie szablonów raportów,

b. umożliwiać przydzielanie uprawnień do szablonów raportów,

c. umożliwiać eksport raportów do pliku w formacie, co najmniej: PDF, RTF, ODT, XML, CSV, TXT, HTML, XLS, DOC, DOCX,

d. umożliwiać generowanie raportu danych osobowych zgodnie z Rozporządzeniem 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 (z Dz. U. 2004 nr 100 poz. 1024 z późn. zm.).

5. Źródłem danych wykorzystywanym w edytorze szablonów raportów powinna być baza danych systemu.

6. System powinien umożliwiać wydruk wygenerowanego raportu.

7. System powinien umożliwiać generowanie raportów dotyczących spraw dla dowolnie wybranych przedziałów czasu i klas z wykazu akt.

Poczta elektroniczna:

1. System powinien posiadać wbudowanego klienta poczty elektronicznej.

2. Klient poczty elektronicznej powinien umożliwiać co najmniej: wysyłanie (protokół SMTP), odbieranie (protokół POP3 lub IMAP), przekazywanie dalej i odpowiadanie na przychodzące wiadomości.

3. Klient poczty elektronicznej powinien umożliwiać załączanie dowolnych plików do wiadomości wychodzącej.

4. Klient poczty elektronicznej powinien umożliwiać określenie adresatów bezpośrednich, adresatów kopii wiadomości oraz kopii ukrytej dla każdej wiadomości wychodzącej.

5. Klient poczty elektronicznej powinien umożliwiać obsługę szyfrowania SSL.

6. System powinien umożliwiać rejestrację wiadomości e-mail z wbudowanego klienta poczty elektronicznej na dwa sposoby w zależności od uprawnień użytkownika. Dla użytkowników obsługujących swoje skrzynki imienne umożliwia automatyczną rejestrację w systemie do dalszego procedowania na koncie użytkownika prowadzącego sprawę. Dla użytkowników obsługujących skrzynki wydziałowe/urzędowe umożliwia automatyczną rejestrację w systemie do przejścia przez ścieżkę dekretacji.

7. Klient poczty elektronicznej powinien umożliwiać sygnowanie załączników podpisem elektronicznym.

8. System powinien umożliwiać rejestrację przesyłek wpływających poczty elektronicznej bezpośrednio z wbudowanego klienta poczty elektronicznej. Rejestracja tych przesyłek powinna polegać na dołączeniu do metadanych opisujących przesyłkę naturalnego dokumentu elektronicznego wraz z załącznikami, w ten sposób aby zachować oryginalną postać i format wiadomości i załączników.

9. System powinien umożliwiać wysyłkę poczty elektronicznej bezpośrednio ze sprawy, której ta przesyłkę dotyczy.

Pozostałe funkcjonalności:

1. System w zakresie dokumentów, korespondencji, spraw powinna pracować zgodnie z Instrukcją Kancelaryjną.

2. System powinien umożliwiać rozproszoną rejestrację wszelkiej korespondencji każdego typu wpływającej do Zamawiającego wraz z załącznikami oraz jej automatyczne numerowanie i oznaczanie kodem kreskowym oraz tworzenie raportów.

3. System powinien udostępniać użytkownikom urzędu jedną wspólną książkę teleadresową z danymi pracowników urzędu, generowaną na podstawie danych ze słownika użytkowników i ze struktury organizacyjnej.

4. System powinien pozwalać na wprowadzanie, gromadzenie, udostępnianie i wyszukiwanie dokumentów niezależnie od mechanizmów i zasad rządzących obiegiem dokumentów. W odniesieniu do takich dokumentów System powinien umożliwiać opisanie za pomocą przypisanej (uprzednio zdefiniowanych) metadanych dokumentu, słów kluczowych oraz umieszczenie w drzewiastej strukturze katalogów.

5. Dostęp użytkowników do dokumentów wprowadzonych niezależnie od mechanizmu obiegu dokumentów powinien być regulowany uprawnieniami.

6. System powinien automatycznie sprawdzać poprawność wprowadzanych do systemu danych typu np. NIP, PESEL, REGON (tzw. walidacja).

7. System powinien posiadać jednolity terminarz organizacji z możliwością wpisywania terminów i rocznic poszczególnym użytkownikom i grupom pracowników oraz ich powiadamiania.

8. System może gromadzić pliki (pliki załączników do dokumentu elektronicznego, odwzorowania cyfrowe zeskanowanych dokumentów) w dowolnych strukturach katalogowych, dając możliwość udostępnienia ich np. organom kontrolującym. W przypadku zastosowania przez Wykonawcę repozytorium plikowego przechowującego pliki w strukturze katalogowej np. systemu operacyjnego, system powinien zapewnić: integralność repozytorium plikowego z wykorzystywaną relacyjną bazą danych oraz zasady bezpieczeństwa i dostępu do danych gromadzonych w repozytorium plikowym.

9. System powinien umożliwiać wprowadzenie początkowych numerów startowych dla wszystkich spisów spraw oraz rejestrów, od których wraz startem aplikacji zaczyna się numerowanie w formie elektronicznej.

10. System jednoznacznie powinien identyfikować użytkownika. Wszystkie operacje zapisywane w historii, w logach aplikacji muszą być przyporządkowane do konkretnego użytkownika nawet, jeśli pracuje w zastępstwie.

11. System powinien udostępniać użytkownikom pomoc kontekstową, tj. funkcję dostępną w każdym widoku aplikacji, wywoływaną na żądanie użytkownika i udostępniająca treść pomocy w kontekście wykonywanych wykorzystywanych funkcji.

Wdrożenie elektronicznego systemu obiegu dokumentów.

Wdrożenie systemu obejmie:

1. Instalację i konfigurację systemu przy uzgodnieniu z Zamawiającym, wymaga się by oprogramowanie było zainstalowane na infrastrukturze Zamawiającego.
2. Instruktaże oraz asystę stanowiskową dla administratora systemu polegająca na:

1) przeprowadzeniu instruktażu obsługi całego systemu bądź jego części wspomagającego obsługę
obszarów działalności urzędu dla wskazanych przez urząd pracowników,
2) przeprowadzeniu we współpracy z każdym wskazanym przez urząd pracownikiem analizy stanowiskowej zadań realizowanych w systemie charakterystycznych dla konkretnych merytorycznych stanowisk pracowniczych,
3) przeprowadzeniu instruktażu w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych systemu dla osób pełniących obowiązki administratorów systemu wskazanych przez urząd.

3. Przeprowadzenie testów penetracyjnych systemu polegających na:

1) przeprowadzeniu testów przeprowadzonych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz (poprzez urządzenie łączące system informatyczny), mających na celu zidentyfikowanie możliwości przeprowadzenia włamania z zewnątrz,
2) badaniu luk dostarczanych systemów informatycznych,
3) identyfikację podatności systemów i sieci na ataki typu: DoS, DDoS, Sniffing, Spoffing, XSS, Hijacking, Backdoor, Flooding, Password, Guessing,
4) sporządzeniu raportu zawierającego minimum: opis stanu faktycznego bezpieczeństwa wdrażanego systemu informatycznego, opis wyników przeprowadzonych testów, rekomendacje dla przyszłych działań związanych z użytkowaniem wdrażanego systemu w kontekście bezpieczeństwa systemu.

4. Zapewnienie opieki powdrożeniowej systemu w okresie trwania projektu (tj. do dnia podpisania końcowego protokołu odbioru całego przedmiotu zamówienia przez Zamawiającego) polegającej na:

1) świadczeniu pomocy technicznej,
2) świadczeniu usług utrzymania i konserwacji dla dostarczonego oprogramowania,
3) dostarczaniu nowych wersji oprogramowania będących wynikiem wprowadzenia koniecznych zmian w funkcjonowaniu systemu związanych z wejściem w życie nowych przepisów,
4) dostosowaniu do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że, zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie,
5) dostarczaniu nowych, ulepszonych wersji oprogramowania lub innych komponentów systemu będących konsekwencją wykonywania w nich zmian wynikłych ze stwierdzonych niedoskonałości technicznych,
6) dostarczaniu nowych wersji dokumentacji użytkownika oraz dokumentacji technicznej zgodnych co do wersji jak i również zakresu zaimplementowanych i działających funkcji

z wersją dostarczonego oprogramowania aplikacyjnego,
7) świadczeniu telefonicznie usług doradztwa i opieki w zakresie eksploatacji systemu.
8) podejmowaniu czynności związanych z diagnozowaniem problemów oraz usuwaniem przyczyn nieprawidłowego funkcjonowania dostarczonego rozwiązania.
Po wdrożeniu Wykonawca przekaże Zamawiającemu wszelkie niezbędne dokumenty w celu umożliwienia mu korzystania z wdrożonego oprogramowania. Dokumenty jakie powinny zostać przekazane to:
1. Pełna dokumentacja powykonawcza obejmująca:
1) opis użytych bibliotek (funkcji, parametrów),
2) szczegółowy schemat baz danych systemu, uwzględniający powiązania i zależności między tabelami,
3) opis techniczny procedur aktualizacyjnych,
4) dostarczenie wszelkich niezbędnych materiałów uzupełniających do powyższej dokumentacji powykonawczej, które są konieczne do właściwej eksploatacji systemu.
2. Instrukcje użytkownika i administratora wdrożonego systemu informatycznego.
3. Raport z przeprowadzonych testów penetracyjnych dla wdrożonego systemu informatycznego.

Wykonawca zobowiązany jest uruchomić testową instancję aplikacji EOD (z testową bazą danych – możliwa w wersji darmowej serwera SQL).

Zakres 5 - Dostawa i wdrożenie Portalu e-Usług wraz z formularzami elektronicznymi

Centralna platforma e-usług mieszkańca to portal integrujący wszystkie dane z innych systemów, informacje o świadczonych e-usługach przez ePUAP, spersonalizowane dane podatkowe. Jest to główny system funkcjonalny z punktu widzenia mieszkańca działający na styku Klient - Urząd. Dzięki niemu mieszkańcy będą mieli dostęp do wszystkich produktów wytworzonych w ramach projektu.

Modernizacja Systemów Dziedzinowych

W ramach modernizacji istniejącego systemu dziedzinowego (poszczególnych modułów) Wykonawca przeprowadzi niezbędne prace programistyczne obejmujące:

1. Przygotowanie systemu dziedzinowego do pełnej obsługi dokumentów elektronicznych sporządzonych przy pomocy formularzy elektronicznych bez konieczności ręcznego wprowadzania dokumentu elektronicznego oraz danych z dokumentu elektronicznego.

2. Utworzenie niezbędnych do procedowania e-usług elementów systemu dziedzinowego.

3. Przygotowanie systemu dziedzinowego w zakresie umożliwienia przygotowania dokumentu elektronicznego w celu wysyłki do klienta bez konieczności ręcznego wprowadzania danych do dokumentu wychodzącego, które istnieją w systemie dziedzinowym.

4. Przygotowanie systemu dziedzinowego w zakresie umożliwienia podpisania dokumentu elektronicznego podpisem kwalifikowanym oraz weryfikacji poprawności podpisu na dokumencie elektronicznym przychodzącym.

5. Przygotowanie systemu dziedzinowego w zakresie umożliwienia automatycznej obsługi dokumentów elektronicznych przychodzących i wychodzących w zakresie innych systemów merytorycznych funkcjonujących w urzędzie.

6. Utworzenie hurtowni danych zawierającej jednolitą i uporządkowaną informację dotyczącą wszystkich należności, wartości odsetek należnych dla urzędu w przypadku należności zaległych ze wszystkich systemów merytorycznych funkcjonujących w urzędzie. Hurtownia danych powinna zawierać rodzaje należności, historię wpłat dotycząca należności wraz z listą osób wpłacających należności, wartości odsetek należnych dla urzędu w przypadku należności zaległych.

7. Przygotowanie systemu dziedzinowego do współpracy z zamawianym systemem elektronicznego obiegu dokumentów (EOD) w zakresie:

1) SD musi mieć możliwość korzystania ze wspólnych danych logowania (login i hasło) z EOD dla pracowników JST opartych o usługę katalogową LDAP,

2) SD musi mieć możliwość synchronizowania baz kontrahentów w zakresie z EOD:

a) dodawania kontrahentów z pełnymi danymi (m.in.: imię, nazwisko/nazwa, pesel, nip, adresy pocztowe, adresy elektroniczne i inne),

b) usuwanie kontrahentów,

c) modyfikowanie danych kontrahenta,

d) masowe synchronizowanie baz kontrahentów,

e) łączenie kontrahentów w obu systemach jednocześnie.

3) Zakres wymienianych danych z EOD nie może być mniejszy niż (w zakresie jakim dotyczy): Nazwisko lub nazwa firmy, Imię, Drugie imię, PESEL, REGON, NIP, Adres stały ze wskazanie na TERYT, Adres korespondencyjny ze wskazaniem na TERYT, Adres skrytki ePUAP, Oznaczenie czy jest zgoda na komunikację drogą elektroniczną, Forma prawna, Typ podmiotu (osoba fizyczna, podmiot gospodarczy).

4) SD musi wymieniać dokumenty elektroniczne przychodzące z ePUAP i skierowane na ePUAP z EOD w zakresie:

a) metadanych dokumentów,

b) dokumentu elektronicznego w XML,

c) załączników do dokumentu elektronicznego.

5) SD musi mieć możliwość podglądu wszystkich dokumentów danego kontrahenta

8. Integracja systemu dziedzinowego w zakresie gospodarki nieruchomościami z zasobem ewidencji gruntów i budynków (z wykorzystaniem formatu plików SWDE), do generowania bazy nieruchomości, a także do celów weryfikacji w systemach dziedzinowych np. porównywania

zgłoszonych powierzchni do opodatkowania a faktycznym stanem posiadania zawartym w ewidencji gruntów i budynków.

9. Integrację systemu dziedzinowego z aplikacjami zewnętrznymi, które pośredniczą w komunikacji z innymi organami administracji np. Zakładem Ubezpieczeń Społecznych (ZUS – program PŁATNIK), Ministerstwem Finansów (MF – BESTIA), oraz Głównym Urzędem Statystycznym (GUS), które agregują dane w skali całego kraju dla celów analitycznych i sprawozdawczych.

10. Integrację systemu dziedzinowego z systemami bankowymi, w zakresie generowania przelewów do banku oraz automatyzacja obsługi wyciągów bankowych, zwłaszcza w zakresie masowych płatności podatników.

11. Przygotowanie mechanizmów integracji z CPeUM poprzez rozbudowę funkcjonalności SD w zakresie:

1) SD musi udostępniać informacje o kontrahentach w zakresie nie mniejszym niż: Nazwa/Nazwisko, Imię, Pesel, NIP, Adres z uwzględnieniem wskazań na słownik TERYT,

2) SD musi udostępniać informacje o należnościach kontrahenta z uwzględnieniem, że kilku kontrahentów może dotyczyć jedna należność,

3) Informacje dot. należności nie mogą mieć mniejszego zakresu niż: rodzaj należności, kwota, kwota do zapłaty, kwota odsetek, VAT, kwota do zapłaty VAT, numer decyzji urzędowej, termin płatności,

4) SD musi udostępniać informacje dotyczące kont bankowych, na które należy wpłacić należność z uwzględnieniem konfiguracji modułu SD dotyczącego przyjmowania masowych płatności,

5) SD musi udostępniać informacje dotyczące wpłat dokonanych na należności. Przekazane dane muszą zawierać zakres informacyjny przynajmniej: data wpłaty, kwota, kwota odsetek, kwota vat, kontrahent wpłacający,

6) SD musi udostępniać szczegółowe informacje dla należności do zapłaty będących Wezwaniami lub Upomnieniami takie jak: data odbioru, data wydania, data zapłaty, koszt, numer,

7) SD musi udostępniać szczegółowe informacje dla należności dotyczących obszaru wydawania zezwoleń na sprzedaż alkoholu w zakresie nie mniejszym niż: data od – do dla zezwolenia, data wydania, numer zezwolenia, rok zezwolenia, typ zezwolenia (A, B, C), stan zezwolenia, adres punktu sprzedaży,

8) SD musi udostępniać szczegółowe informacje dla należności dotyczących mienia, w zakresie nie mniejszym niż: data wystawienia dokumentu, numer dokumentu, nazwa dokumentu (np. Akt notarialny, Akt własności ziemi, decyzja administracyjna, księga wieczysta i inne), dane o nieruchomości której to dotyczy (lokal, budynek, działka, obręb, jednostka ewidencyjna), dane kontrahenta wskazanego jako właściciel i część udziału którą posiada (np. 100%, 1/3, etc.),

9) SD musi udostępniać informacje dla należności dotyczącej podatku od osób prawnych i fizycznych w zakresie nie mniejszym niż: numer dokumentu, rok dokumentu, typ dokumentu (Decyzja czy Deklaracja), rodzaj podatku, typ decyzji, wskazanie nieruchomości które dotyczy (budynek, działka, obręb etc.),

10) SD musi udostępniać informacje dla należności dotyczącej opłaty za gospodarowanie odpadami w zakresie minimalnym: punkt odbioru odpadów, typ zbiórki odpadów (np. selektywna / nieselektywna), parametry deklaracji, numer deklaracji, adres punktu odbioru odpadów.,

11) SD musi udostępniać informacje o mieszkańcach tj. dane kontrahenta dodatkowo uzupełnione o datę urodzenia / zgonu, płeć, adres zameldowania z terenu JST,

12) SD musi umożliwiać podanie należności z określeniem: nazwy, typu, kwoty, terminu płatności, kontrahenta,

13) CPeUM i SD muszą mieć możliwość korzystania z jednego systemu LDAP, który pozwoli na posługiwanie się jednym loginem i hasłem dla pracowników JST.

Po przeprowadzonych pracach programistycznych system dziedzinowy powinien osiągnąć następujące funkcjonalności:

1. Baza informacji o interesantach urzędu, powinna być jedna i wspólna dla wszystkich modułów dziedzinowych.

2. Baza informacji o kontrahentach powinna mieć możliwość podziału na grupy lub jednostki, tak aby użytkownik z jednej jednostki nie miał dostępu do danych osobowych z drugiej jednostki.

3. System powinien mieć możliwość archiwizacji dokumentów, danych.

4. System powinien obsługiwać płatności masowe i automatyczne księgowanie wyciągów bankowych.

5. Wszystkie moduły podatkowe powinny mieć wspólne słowniki (stawek podatkowych, rodzaju i stawek ulg, obrębów ewidencyjnych itp.), oraz być zintegrowane, tak by organizacyjnie osoba merytoryczna wystawiająca np. zaświadczenie dla podatnika o zaleganiu bądź niezaleganiu w podatkach miała dostęp do grupy funkcji wydawania zaświadczeń obejmujących wszystkie moduły podatkowe. Podobnie w zakresie wydawania decyzji umarzających, zmieniających terminy płatności, rozkładających należność na raty, symulacjami i postępowaniem egzekucyjnym. System powinien dawać możliwość ustawienia wielu wartości słownikowych w jednym miejscu, np. słownik stawek, terminów, klas gruntów itp.

6. Moduły dziedzinowe powinny być zintegrowane z modułami usług dla ludności, a w szczególności, w zakresie przelewów masowych (w księgowości zobowiązań powinno być widoczne, na które należności dokonano przelewów), dokumentów elektronicznych składanych przez interesantów za pomocą platformy ePUAP i dostępnych formularzy (np. deklaracji czy informacji podatkowych).

7. Wymagana jest możliwość zapisu szablonów systemowych do wydruków z systemu dziedzinowego do pliku zewnętrznego (w celu ich dalszej modyfikacji) oraz modyfikacja szablonów wydruków w aplikacji, a także możliwość wydruków z użyciem zmodyfikowanego szablonu (z pliku).

8. Musi być możliwość pracy w środowisku sieciowym z możliwością jednoczesnego dostępu do danych wielu użytkownikom.

9. Musi istnieć mechanizm zapewniający bezpieczeństwo danych oraz mechanizmy autoryzacji przez logowanie do aplikacji (także z wykorzystaniem uwierzytelniania za pomocą usług katalogowych).

10. Dostęp (zabezpieczony hasłem i kodem dostępu) do poszczególnych modułów musi być możliwy przez wyposażenie w funkcje zarządzania użytkownikami modułów (przydzielania lub odbieranie uprawnień do poszczególnych funkcji lub grupy funkcji, a także aktywowanie lub zamykanie kont użytkowników).

11. W bazie danych musi być zapis informacji o dodaniu rekordu (data i godzina operacji, użytkownik) oraz o ostatniej modyfikacji rekordu (data i godzina operacji, użytkownik).

12. Na każdym etapie pracy użytkowników poszczególnych modułów merytorycznych musi istnieć tzw. pomoc kontekstowa informująca użytkownika o możliwych działaniach.

13. System powinien dawać możliwość wymuszania zmiany hasła, aby użytkownicy musieli zmieniać hasło w określonym odstępie czasu. System musi też umożliwiać skonfigurowanie wymuszania stosowania tzw. twardego hasła, np. wymuszając stosowanie wielkich i małych liter, cyfr itp.

14. System powinien zabezpieczać przed nieautoryzowanym dostępem do bazy danych.

15. System powinien mieć możliwość wykonywania kopii zapasowej bazy danych z poziomu systemu, bez konieczności dostępu do bazy danych na serwerze.

16. System powinien dawać możliwość skorzystania z tzw. „zdalnego pulpitu", aby użytkownicy mogli się łączyć zdalnie z pracownikiem wsparcia systemu.

17. Zarządzanie uprawnieniami powinno umożliwiać również ograniczenie uprawnień do danej jednostki budżetowej. Przykładowo użytkownik obsługujący moduł księgowy powinien mieć uprawnienia jedynie do jednostki, którą obsługuje.

18. Powinna istnieć możliwość wysyłania przez administratora systemu komunikatów do poszczególnych użytkowników, jak również wylogowanie użytkownika z systemu.

19. Powinna być możliwość ustawienia wielu jednostek organizacyjnych, aby zwiększyć możliwość pracy kontekstowej i umożliwiać np. dodanie różnych pieczątek dla różnych jednostek, różnych numerów NIP itp.

20. System powinien dawać administratorowi możliwość zarządzania listą aktywnych modułów i funkcji. Zarządzanie powinno dawać możliwość aktywacji, dezaktywacji modułu lub funkcji.

21. System musi dawać możliwość ustawienia parametrów czasu bezczynności. Po określonym czasie nieużywania systemu użytkownik musi być wylogowany z systemu.

22. Mechanizm wspólnej bazy danych musi zabezpieczać przed powielaniem zapisów, np. blokować możliwość ręcznego wpisywania nazwy ulicy przez użytkownika i wymuszać używanie słowników.

23. System w przypadku aktywnego modułu do obsługi ewidencji ludności powinien dawać możliwość aktualizowania danych wprowadzanego kontrahenta danymi z ewidencji ludności.

24. System powinien kontrolować, aby użytkownicy wykonujący operacje na tych samych danych nie mogli tego wykonać. System musi blokować operacje użytkownika, który chce wykonać działanie na modyfikowanych danych. Blokada powinna być zdejmowana przez administratora systemu.

25. System musi dawać możliwość kontrolowania połączeń systemu z bazą danych oraz dawać możliwość sprawdzania dostępności nowych wersji systemu.

26. Powinna istnieć możliwość konfiguracji i kontroli integracji z innymi systemami. Administrator w jednym miejscu powinien mieć możliwość sprawdzenia konfiguracji z innymi systemami, a także ustawienia listy elementów podlegających integracji (kontrahenci, dokumenty itp.).

27. System powinien dawać możliwość eksportu danych do formatu XML i CSV dla ustalonych parametrów indywidualnie przez użytkownika.

28. System powinien umożliwiać wyszukanie listy wykonanych eksportów wg. zadanych parametrów.

29. System powinien dawać możliwość tworzenia pliku IPE-PN XML dla osób prawnych i fizycznych dotyczący danych podatkowych.

30. Powinna istnieć możliwość eksportu danych w formacie XML z modułu rejestru mieszkańców oraz modułów podatkowych.

31. System musi być bezpieczny, to znaczy musi posiadać procedury ochrony i kontroli dostępu do całej bazy danych (ochrona przed nieuprawnionym dostępem, mechanizmy kryptograficzne, wsparcie redundancji sprzętowej i programowej, ochrona integralności danych, zabezpieczenie danych przed uszkodzeniem i utratą danych), oraz poszczególnych rodzajów danych (np. dane osobowe, dane o zaległościach podatników). Dostęp do bazy musi być zabezpieczony zakodowanym hasłem i odpowiednio zdefiniowanymi parametrami połączenia aplikacji z bazą.

32. System musi umożliwiać elastyczne zarządzanie użytkownikami i uprawnieniami to znaczy:

1) aktywowanie oraz dezaktywowanie (bez usuwania) kont użytkowników,

2) możliwość podglądu aktualnie zalogowanych użytkowników,

3) przypisywanie (lub odbieranie) uprawnień dla użytkowników do poziomu jednostkowej funkcji,

4) grupowanie dowolnie wybranych funkcji w zbiory uprawnień (grupy funkcji) i przypisywanie (lub odbieranie) ich użytkownikom,

5) brak możliwości zmiany danych historycznych,

6) możliwość zmiany hasła użytkownika oraz jego resetowania, wymuszanie zmiany hasła co 30 dni zgodnie z ogólnymi wymaganiami dotyczącymi systemów informatycznych,

7) umożliwienie identyfikowania użytkownika po nr PESEL oraz nazwie użytkownika.

33. Moduły obsługujące prowadzenie rozliczeń finansowych podatników i płatników urzędu, powinny być pogrupowane według różnych rodzajów należności i jednocześnie powinny stanowić wzajemnie spójną całość, tak by użytkownik aplikacji, w zależności od nadanych mu uprawnień,

mógł mieć możliwość obsługi wybranego konta zobowiązanego z dostępem do jego wszystkich zobowiązań wobec urzędu (System musi mieć możliwość dokonywania przeksięgowań np. z należności podatkowej na inną nie podatkową, automatyczne rozdysponowanie wpłaty na występujące należności).

34. System musi umożliwiać wysyłanie wiadomości w zakresie minimalnym o: informacji o wystawionej decyzji; informacji o zbliżającym się terminie płatności; informacji o zaległości; wezwania do złożenia deklaracji;

Zamawiający nie posiada autorskich praw majątkowych do funkcjonującego w urzędzie oprogramowania, nie posiada kodów źródłowych oprogramowania, a licencja posiadanego oprogramowania nie umożliwia mu modyfikacji kodów źródłowych, zatem Zamawiający nie jest w stanie zapewnić Wykonawcę, że udostępni mu stałe, niezmienne interfejsy integracyjne umożliwiające pełną wymianę danych z nowo uruchamianymi rozwiązaniami. Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp.

Mając na uwadze powyższe, w przypadku jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności postępowania, Zamawiający dopuszcza wymianę systemu dziedzinowego na jedno zintegrowane rozwiązanie (Zintegrowany System Dziedzinowy- ZSD) pod warunkiem, że:

1. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt, z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.

2. Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, migracja musi objąć pełny zakres danych bieżących i archiwalnych.

3. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę systemów.

4. Wymiana systemu nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.

W szczególności dotyczy to wymiaru podatków i opłat, sprawozdawczości budżetowej oraz obsługi kadrowo-płacowej.

5. Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.

6. Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.

7. Nowe rozwiązania muszą realizować wszystkie wymienione wyżej funkcje systemu oraz zapewnić zgodność z wymaganiami dla systemu dziedzinowego określonymi poniżej.

Wymogi funkcjonalne dla zintegrowanego systemu dziedzinowego ofertowanego jako rozwiązanie równoważne do modernizacji istniejącego systemu dziedzinowego.

Zintegrowany System Dziedzinowy (ZSD) musi objąć cały obszar funkcjonalny Zamawiającego z wyłączeniem zadań realizowanych przez systemy krajowe (np. CEIDG, Bestia@). Zintegrowany System Dziedzinowy musi być przygotowany do pełnej obsługi dokumentu elektronicznego tj. musi umożliwiać przyjęcie danych poprzez import danych z dokumentów elektronicznych sporządzonych przy pomocy formularzy elektronicznych udostępnionych przez Zamawiającego, bez konieczność ręcznego wprowadzania danych z dokumentu elektronicznego. Zintegrowany System Dziedzinowy musi umożliwić przygotowanie dokumentu elektronicznego w celu wysyłki go do klienta oraz wydrukowanie kopii dokumentu w wersji papierowej zgodnie z wymaganiami Instrukcji Kancelaryjnej.

Wszystkie funkcjonalności muszą umożliwiać pełną realizację czynności niezbędnych do obsługi danego obszaru. Funkcjonalności muszą być ergonomiczne, wykonane zgodnie z najlepszymi praktykami projektowania systemów informatycznych.

Zaleca się, aby ZSD miał budowę modułową oraz zapewniał pełną wymianę informacji pomiędzy poszczególnymi modułami systemu pozwalając na kompletne i kompleksowe prowadzenie wszystkich zadań administracji samorządowej, jednak Zamawiający nie narzuca sposobu podziału ZSD na moduły, czy ich liczby. Z punktu widzenia Zamawiającego istotnym jest spełnienie przez ZSD wskazanych niżej funkcjonalności. W stosunku do Zintegrowanego Systemu Dziedzinowego na potrzeby opisu funkcjonalnego stosuje się zamiennie nazwy: „moduł" – mając na uwadze część funkcjonalną Zintegrowanego Systemu Dziedzinowego, „obszar" – mając na uwadze część funkcjonalną Zintegrowanego Systemu Dziedzinowego, a także „System", „Aplikacja" – mając na uwadze ZSD.

W przypadku, jeżeli Zamawiający nie uwzględnił obszaru funkcjonalnego systemu ZSD w poniższym opisie, a jest on niezbędny z tytułu funkcjonowania całego rozwiązania oraz e-usług publicznych musi on zostać uwzględniony przez Wykonawcę w cenie oferty, a wszystkie dostarczone elementy ZSD muszą spełniać wymogi licencyjne określone w niniejszym dokumencie.

W szczególności platforma e-usług zawierać powinna:

1. Opisy wszystkich usług świadczonych przez urząd na platformie ePUAP, z których mieszkaniec

może skorzystać w sposób elektroniczny;

2. Możliwość śledzenia postępu swoich spraw;

3. Podgląd swoich, spersonalizowanych danych o należnościach i zobowiązaniach z tytułu podatków i opłat lokalnych;

4. Możliwość dokonania płatności z tytułu podatków i opłat lokalnych;

5. Możliwość umówienia się na wizytę w Urzędzie.

Wymagania funkcjonalne centralnej platformy e-usług mieszkańca:

1. Portal musi umożliwiać bezpieczne zalogowanie się przez przeglądarkę z wykorzystaniem SSO (Single Sign-On) platformy ePUAP (protokół SAML).

2. Portal musi umożliwiać pozyskiwanie z Systemu Dziedzinowego (dalej SD), modernizowanego w ramach niniejszego projektu, danych o aktualnych zobowiązaniach zalogowanego interesanta z uwzględnieniem należności dodatkowych tj. odsetki i inne koszty na bieżącą datę logowania w zakresie:

1) prowadzenia spraw w zakresie podatku od nieruchomości od osób fizycznych,

2) prowadzenia spraw w zakresie podatku od nieruchomości od osób prawnych,

3) prowadzenia spraw w zakresie podatku rolnego od osób fizycznych,

4) prowadzenia spraw w zakresie podatku rolnego od osób prawnych,

5) prowadzenia spraw w zakresie podatku leśnego od osób fizycznych,

6) prowadzenia spraw w zakresie podatku leśnego od osób prawnych,

7) prowadzenia spraw w zakresie podatku od środków transportowych,

8) prowadzenia spraw w zakresie opłat za gospodarowanie odpadami komunalnymi,

3. Portal musi zawierać elektroniczne biuro interesanta stanowiące wirtualny punkt przyjęć formularzy elektronicznych stosowanych w urzędzie oraz informacji dotyczących sposobu załatwienia spraw, co najmniej w zakresie odpowiadającym e-usługom wdrażanym w ramach zamówienia.

4. Portal w części publicznej musi prezentować skategoryzowane karty usług.

5. Portal musi być podzielny na część publiczną – udostępnianą niezalogowanym użytkownikom i użytkownikom zalogowanym do portalu oraz część wewnętrzną – dla administratora systemu i pracowników urzędu.

6. Użytkownik w części publicznej powinien mieć możliwość przejrzenia karty usługi, dla której prezentowanej jest opis zredagowany przez administratora oraz możliwość przejścia do wypełnienia formularza elektronicznego na ePUAP.

7. Karta usługi powinna być charakteryzowana przynajmniej przez następujące atrybuty: nazwę, opis, do kogo jest skierowana (obywatel - czyli usługi typu A2C, przedsiębiorcy - czyli usługi typu A2B, instytucji/urzędu – czyli usługi typu A2A).

8. Administrator musi mieć możliwość zdefiniowania karty usługi i utworzenia jej wizualizacji.

9. Wszystkie dane muszą być pobierane z SD.

10.System musi umożliwiać zarządzanie rejestrem interesantów, gdzie każdego interesanta można:

1) zidentyfikować minimum takimi danymi jak: typ podmiotu, Imię, Nazwisko, Login, dane kontaktowe (telefon, e-mail, faks, www, adres korespondencyjny, oraz dowolną liczbę innych form kontaktu),

2) zmienić mu dane podstawowe,

3) zmienić mu dane kontaktowe,

4) powiązać go z interesantem z SD,

5) aktywować konto interesanta,

6) przypisać interesanta do grup użytkowników.

11.Administrator musi mieć możliwość powiązania użytkownika z jednym lub kilkoma kontami kontrahenta w SD.

12.Użytkownik zalogowany do systemu musi mieć możliwość przeglądania i zmiany własnych danych: typ podmiotu (osoba fizyczna / osoba prawna), imię, nazwisko / nazwa, dane kontaktowe standardowe: telefon, email, fax, www, adres korespondencyjny, dane kontaktowe dodatkowe.

13.Użytkownik musi mieć możliwość zmiany hasła.

14.Użytkownik musi mieć możliwość powiązania konta z kontem ePUAP.

15.Użytkownik musi mieć możliwość odłączenia konta od ePUAP.

16.Użytkownik musi mieć możliwość przeglądu swoich danych kontrahenta z SD, o ile jego konto zostało powiązane z kontem kontrahenta SD.

17.Dane podstawowe prezentowane w przypadku powiązania konta z kontrahentem SD to co najmniej: nazwisko imię / nazwa, typ, PESEL, NIP, data wyrejestrowania lub zgonu (jeśli widnienie w SD).

18.O ile konto powiązane jest z SD, system musi prezentować dla danego użytkownika:

1) dane zameldowania, o ile użytkownik jest zameldowany na terenie JST,

2) listę nieruchomości, gdzie dla każdej nieruchomości prezentowana jest wielkość, typ nieruchomości, typ własności lista opłat i podatków pobieranych z tytułu nieruchomości: m.in.: podatek od osób fizycznych, podatek od osób prawnych, opłaty za gospodarowanie odpadami komunalnymi,

3) listę środków transportu – podlegającą opłatom o ile w SD użytkownik jest podmiotem prawnym posiadającym opodatkowane środki transportu,

4) listę dokumentów z rozdzieleniem na dokumenty wpływające do JST oraz wychodzące z JST dla zalogowanego użytkownika w zakresie e-usług,

5) listę opłat lokalnych (skarbowe, opłaty za pas drogowy, koncesje alkoholowe oraz inne opłaty),

6) listę faktur do zapłaty o ile dotyczy.

19.Po zalogowaniu na swoje konto interesant musi mieć możliwość wyświetlenia informacji o wszystkich swoich należnościach wobec JST pobranych z SD oraz historię swoich płatności. Portal musi umożliwiać przegląd wszystkich zobowiązań finansowych z uwzględnieniem tytułu należności, należności głównej, odsetki, koszty upomnień, wezwań do zapłaty, salda do zapłaty, terminie płatności, kwocie już zapłaconej (w przypadku należności, która została już częściowo spłacona), kwocie zleconej płatności poprzez portal oraz dacie i godzinie zlecenia tej płatności.

20.Każda należność powinna zawierać co najmniej takie informacje jak: numer decyzji, naliczone odsetki oraz koszty upomnień i wezwań, czy był na nią wystawiony tytuł wykonawczy itp.

21.Możliwość prezentowania i wyszukiwania konkretnej należności według rodzaju, daty, terminu płatności itp.

22.Jeżeli należność została dopiero częściowo spłacona to użytkownik musi mieć możliwość otrzymania pełnej informacji w układzie: ile było wpłat na daną należność, kwota każdej płatności, data płatności oraz informację czy płatność została już zaksięgowana czy nie i saldo do zapłaty.

23.Możliwość wyświetlania historii wszystkich interakcji finansowych mieszkańca z urzędem, jakie zostały zrealizowane poprzez system.

24.System powinien być zintegrowany co najmniej z dwoma systemami płatniczymi. Systemy płatnicze powinny posiadać zezwolenie Komisji Nadzoru Finansowego na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej lub realizować bezpośrednie płatności z konta płatnika na rachunek urzędu.

25.Aplikacja musi pozwalać na wnoszenie opłat za pośrednictwem systemu płatności elektronicznych w różny sposób tzn. przez wygenerowanie płatności na wybraną należność i opłacenie, lub na zaznaczenie kilku należności i zapłacenie je jednym przelewem.

26.Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów należności.

27.Jeśli należność jest płatna w ratach (np. należności podatkowe, należności rozłożone przez urząd na raty) portal winien również przedstawiać klientowi informację, którą ratę kwota płatności stanowi.

28.W sytuacji, kiedy kilku klientów jest solidarnie zobowiązanych do zapłaty należności klient zalogowany do portalu musi widzieć również minimum imię, nazwisko i adres pozostałych współzobowiązanych. W przypadku podmiotów gospodarczych będzie to nazwa firmy i jej siedziba.

29.W przypadku, jeśli należność powstała w drodze decyzji administracyjnej urzędu numer decyzji ma być również widoczny dla klienta.

30.Możliwość ukrycia wyświetlania wybranych parametrów należności wyszukiwanych na ekranie

użytkownika.

31.Aplikacja powinna posiadać mechanizmy kontroli i bezpieczeństwa chroniące użytkowników przed kilkukrotnym wniesieniem płatności z tego samego tytułu.

32.Portal musi generować komunikaty informujące i/lub ostrzeżenia wizualne dla użytkownika podczas próby ponownego zlecenia płatności dla należności, dla których płatność została zlecona za pośrednictwem portalu a transakcja jeszcze jest przetwarzana.

33.Możliwość wydrukowania wypełnionego polecenia przelewu bankowego lub pocztowego, dla zaznaczonej jednej lub zaznaczonych wielu należności.

34.Możliwość wyszukiwania i prezentowania należności według jej rodzaju np. „pokaż tylko opłaty za dzierżawę" itp.

35.Możliwość wyszukiwania i prezentowania należności według statusu płatności tzn. np. pokaż tylko zaległe itp.

36.Możliwość wysyłania przypomnień o terminie płatności za pośrednictwem sms.

37.Wygenerowane płatności zlecone za pośrednictwem portalu, ale jeszcze nie zaksięgowane powinny zawierać informacje takie jak: nr konta bankowego na które została przelana płatność, kwota i data zlecenia, status zlecenia oraz data wykonania.

38.Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów.

39.Informacje o wygenerowanych płatnościach muszą być przesyłane z portalu do SD. Proces przesyłania danych musi mieć możliwość ustawienia częstotliwości wykonana dla administrator systemu (w zakresie od „raz na dobę" do „co 5 minut").

40.Możliwość wyszukiwania lub filtrowania należności według co najmniej: konta bankowego na które została przelana płatność, rodzaju należności, kwoty, typu płatności, stanu zlecenia, daty zlecenia.

41.Możliwość przeglądu operacji księgowych już zrealizowanych tzn. opłaconych (wpłaty, zwroty, przeksięgowania)

42.Przegląd operacji księgowych już zrealizowanych na należnościach (wpłaty, zwroty, przeksięgowania) z wyszczególnionym dla każdej operacji co najmniej: jej rodzaju, konta bankowego na którym została zaksięgowana operacja, identyfikator, rok, rata, kwota, odsetki, kwota zapłacona faktycznie, data i godzina przelewu.

43.Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów.

44. Możliwość wyszukiwania lub filtrowania zrealizowanych i zaksięgowanych operacji według co

najmniej: kontrahenta SD, rodzaju należności, terminu płatności od – do

45.Dla należności dotyczących nieruchomości system musi prezentować dodatkowo minimum: numer decyzji, typ nieruchomości, numer nieruchomości, numer dokumentu własności/władania, datę wydania dokumentu – pobrane z SD.

46.Dla należności dotyczących podatku od osób prawnych system musi prezentować dodatkowo rok wydania decyzji, typ dokumentu, rodzaj podatku.

47.Dla danych upomnienia system musi prezentować dodatkowo: numer upomnienia, rok upomnienia, koszt upomnienia, datę wydania upomnienia, datę odbioru upomnienia, kwotę do zapłaty.

Wymagania niefunkcjonalne centralnej platformy e-usług mieszkańca:

1. System musi być zaprojektowany w modelu trójwarstwowym:

1) warstwa danych,

2) warstwa aplikacji,

3) warstwa prezentacji - przeglądarka internetowa - za pośrednictwem której następuje właściwa obsługa systemu przez użytkownika końcowego.

2. System powinien umożliwiać pracę na bazie typu Open Source bądź na komercyjnym systemie bazodanowym.

3. System w warstwie serwera aplikacji i bazy danych powinien mieć możliwość uruchomienia w środowiskach opartych na systemach operacyjnych z rodziny Windows lub równoważnych oraz w środowiskach opartych na systemie Linux lub równoważnych.

4. System w warstwie klienckiej powinien poprawnie działać w różnych środowiskach z minimum 5 najbardziej popularnymi przeglądarkami w Polsce w ich najnowszych wersjach (zgodnie ze statystyką prowadzoną na stronie http://gs.statcounter.com/ za okres 6 miesięcy poprzedzających miesiąc ogłoszenia postępowania określoną dla komputerów stacjonarnych „desktop").

5. System powinien realizować wszystkie czynności przez przeglądarkę internetową.

6. System musi pracować w wersji sieciowej z wykorzystaniem protokołu TCP/IP oraz być w pełni kompatybilny z sieciami TCP/IP.

7. Architektura systemu powinna umożliwiać pracę jedno i wielostanowiskową, zapewniać jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników.

8. W przypadku gdy system do pracy wykorzystuje silnik bazy danych, baza taka musi być kompatybilna z systemem operacyjnym i musi istnieć możliwość jej instalacji i pracy na zasadach określonych jak dla systemu.

9. System w zakresie wydruków musi wykorzystywać funkcjonalność systemu operacyjnego i umożliwiać wydruk na dowolnej drukarce zainstalowanej i obsługiwanej w systemie operacyjnym, na którym zostanie zainstalowane oprogramowanie (drukarki lokalne, drukarki sieciowe).

10.Interfejs użytkownika (w tym administratora) powinien być w całości polskojęzyczny.

11.Dokumentacja powinna zawierać opis funkcji programu, wyjaśniać zasady pracy z programem, oraz zawierać opisy przykładowych scenariuszy pracy.

12.Dokumentacja musi być dostępna z poziomu oprogramowania w postaci elektronicznej (pliki PDF

lub DOC lub RTF).

13.System musi zapewniać weryfikację wprowadzanych danych w formularzach i kreatorach.

14.Zapewnienie bezpieczeństwa danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej przy zastosowaniu bezpiecznych protokołów sieciowych.

15.System powinien być skalowalny, poprzez możliwość dołączenia dodatkowych stanowisk komputerowych, zwiększenie zasobów obsługujących warstwę aplikacyjną, zwiększenie zasobów obsługujących warstwę bazy danych.

16.System powinien umożliwiać okresowe wykonywanie, w sposób automatyczny, pełnej kopii aplikacji i danych systemu.

17.System powinien posiadać funkcjonalność zarządzania dostępem do aplikacji:

1) administrator systemu ma możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,

2) administrator systemu powinien móc nadawać uprawnienia użytkownikom,

3) administrator systemu powinien mieć możliwość przypisywać użytkowników do grup,

4) system pozwalać powinien na zmianę danych uwierzytelniających użytkownika.

18.System powinien posiadać możliwość określenie maksymalnej liczby nieudanych prób logowania, po przekroczeniu której użytkownik zostaje zablokowany.

19.System powinien się komunikować z systemami zewnętrznymi w sposób zapewniający poufność danych.

20.System powinien być odporny na znane techniki ataku i włamań, typowe dla technologii, w której został wykonany.

21.Docelowo system powinien być zintegrowany z modułami finansowo-księgowymi i podatkowymi w zakresie niezbędnym do realizacji funkcjonalności e-usług oraz systemem elektronicznego obiegu spraw i dokumentów.

22.System powinien prowadzić dziennik zdarzeń (w postaci logów systemowych) i dostępu do obiektów danych, dokumentów, operacji na słownikach umożliwiający odtwarzanie historii aktywności poszczególnych użytkowników systemu.

23.System musi posiadać stronę główną umożliwiającą dodanie nazwy adresu oraz znaku graficznego JST.

Wdrożenie platformy e-usług mieszkańca.

Wdrożenie systemu obejmie:

1. Instalację i konfigurację systemu przy uzgodnieniu z Zamawiającym, wymaga się by oprogramowanie było zainstalowane na infrastrukturze Zamawiającego.

2. Instruktaże oraz asystę stanowiskową dla administratora systemu polegająca na:

1) przeprowadzeniu instruktażu obsługi całego systemu bądź jego części wspomagającego obsługę obszarów działalności urzędu dla wskazanych przez urząd pracowników,

2) przeprowadzeniu we współpracy z każdym wskazanym przez urząd pracownikiem analizy stanowiskowej zadań realizowanych w systemie charakterystycznych dla konkretnych merytorycznych stanowisk pracowniczych,

3) przeprowadzeniu instruktażu w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych systemu dla osób pełniących obowiązki administratorów systemu wskazanych przez urząd.

3. Przeprowadzenie testów penetracyjnych systemu polegających na:

1) przeprowadzeniu testów przeprowadzonych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz (poprzez urządzenie łączące system informatyczny), mających na celu zidentyfikowanie możliwości przeprowadzenia włamania z zewnątrz,

2) badaniu luk dostarczanych systemów informatycznych;

3) identyfikację podatności systemów i sieci na ataki typu: DoS, DDoS, Sniffing, Spoffing, XSS, Hijacking, Backdoor, Flooding, Password, Guessing,

4) sporządzeniu raportu zawierającego minimum: opis stanu faktycznego bezpieczeństwa wdrażanego systemu informatycznego, opis wyników przeprowadzonych testów, rekomendacje dla przyszłych działań związanych z użytkowaniem wdrażanego systemu w kontekście bezpieczeństwa systemu.

4. Zapewnienie opieki powdrożeniowej systemu w okresie trwania projektu (tj. do dnia podpisania końcowego protokołu odbioru całego przedmiotu zamówienia przez Zamawiającego) polegającej na:

1) świadczeniu pomocy technicznej,

2) świadczeniu usług utrzymania i konserwacji dla dostarczonego oprogramowania,

3) dostarczaniu nowych wersji oprogramowania będących wynikiem wprowadzenia koniecznych zmian w funkcjonowaniu systemu związanych z wejściem w życie nowych przepisów,

4) dostosowaniu do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że, zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie,

5) dostarczaniu nowych, ulepszonych wersji oprogramowania lub innych komponentów systemu będących konsekwencją wykonywania w nich zmian wynikłych ze stwierdzonych niedoskonałości technicznych,

6) dostarczaniu nowych wersji dokumentacji użytkownika oraz dokumentacji technicznej zgodnych co do wersji jak i również zakresu zaimplementowanych i działających funkcji z wersją dostarczonego oprogramowania aplikacyjnego,

7) świadczeniu telefonicznie usług doradztwa i opieki w zakresie eksploatacji systemu.

8) podejmowaniu czynności związanych z diagnozowaniem problemów oraz usuwaniem przyczyn nieprawidłowego funkcjonowania dostarczonego rozwiązania.

Po wdrożeniu Wykonawca przekaże Zamawiającemu wszelkie niezbędne dokumenty w celu umożliwienia mu korzystania z wdrożonego oprogramowania. Dokumenty jakie powinny zostać przekazane to:

1. Pełna dokumentacja powykonawcza.

2. Instrukcje użytkownika i administratora wdrożonego systemu informatycznego.

3. Raport z przeprowadzonych testów penetracyjnych dla wdrożonego systemu informatycznego

Dostarczenie i wdrożenie formularzy e-usług

Wykonawca dokona pełnego wdrożenia formularzy elektronicznych na ePUAP w Środowisku Budowy Aplikacji oraz dokona ich integracji z Portalem.

Tabela 1 Parametry minimalne wdrożonych formularzy elektronicznych

Nr.	Wymaganie
4.1.	Formularze stosowane na ePUAP tworzone są z wykorzystaniem języka XForms oraz XPath.
4.2.	Wykonawca opracuje formularze elektroniczne (zgodnie z właściwymi przepisami prawa) na podstawie przekazanych przez JST, których dotyczy przedmiotowe zamówienie, kart usług z formularzami w formacie MS Word.
4.3.	Wszystkie formularze elektroniczne Wykonawca przygotuje z należytą starannością tak, aby pola do uzupełnienia w tych formularzach zgadzały się z polami formularzy w formacie MS Word.
4.4.	Pola wskazane przez Zamawiającego jako pola obowiązkowe w formularzach w formacie MS Word, musza zostać polami obowiązkowymi również w formularzach elektronicznych. Wraz z weryfikacją poprawności wprowadzonych danych (min. format np. PESEL, NIP, REGON, itp.)
4.5.	Układ graficzny wszystkich formularzy powinien być w miarę możliwości jednolity.
4.6.	Wizualizacja formularzy elektronicznych nie musi być identyczna ze wzorem w formacie MS Word, ale musi zawierać dane w układzie niepozostawiającym wątpliwości co do treści i kontekstu zapisanych informacji, w sposób zgodny ze wzorem oraz obowiązującymi przepisami prawa.
4.7.	Przygotowując formularze Wykonawca musi dążyć do maksymalnego wykorzystania słowników.
4.8.	W budowanych formularzach należy wykorzystać mechanizm automatycznego pobierania danych z profilu – celem uzupełnienia danych o wnioskodawcy.
4.9.	Formularze muszą zapewniać walidację wprowadzonych danych po stronie klienta i serwera zgodnie z walidacją zawartą w schemacie dokumentu.
4.10.	Jeśli w formularzu elektronicznym występują pola o ustalonej możliwej wartości (np. PESEL, REGON, kod pocztowy, ulica, miasto), to pola te muszą być walidowane pod kątem poprawności danych wprowadzanych przez wnioskodawcę.
4.11.	Każdy opracowany przez Wykonawcę formularz (w postaci pliku XML) musi zostać przekazany Zamawiającemu na okres 7 dni roboczych w celu dokonania sprawdzenia i wykonania testów na formularzu.
4.12.	Po okresie testów, o których mowa w wymaganiu poprzednim, Zamawiający przekaże Wykonawcy ewentualne poprawki i uwagi dotyczące poszczególnych formularzy, które Wykonawca usunie bez zbędnej zwłoki.

4.13.	Wykonawca przygotuje wzory dokumentów elektronicznych w CRD zgodnie ze standardem ePUAP w formacie XML zgodnym z formatem Centralnego Repozytorium Wzorów Dokumentów.
4.14.	Zamawiający dopuszcza możliwość wykorzystania przez Wykonawcę wzorów, które są już opublikowane w CRD.
4.15.	Wygenerowane dla poszczególnych formularzy wzory dokumentów elektronicznych, składające się z plików: • Wyróżnik (wyróżnik.xml) • Schemat (schemat.xml) • Wizualizacja (styl.xsl) muszą zostać dostosowane do wymogów formatu dokumentów publikowanych w CRD i spełniać założenia interoperacyjności.
4.16.	W ramach projektu Wykonawca przygotuje i przekaże Zamawiającemu wszystkie wzory dokumentów elektronicznych w celu złożenia wniosków o ich publikację w CRD.
4.17.	Wykonawca udzieli wsparcia Zamawiającemu w przejściu procesu publikacji na ePUAP.
4.18.	Bazując na przygotowanych wzorach dokumentów elektronicznych oraz opracowanych na platformie ePUAP formularzach elektronicznych Wykonawca przygotuje instalacje aplikacji w środowisku ePUAP.
4.19.	Aplikacje muszą być zgodne z architekturą biznesową ePUAP oraz architekturą systemu informatycznego ePUAP.
4.20.	Przygotowane aplikacje muszą zostać zainstalowane przez Wykonawcę na koncie ePUAP Zamawiającego.
4.21.	Zainstalowane aplikacje muszą spełniać wymogi ePUAP oraz pozytywnie przechodzić przeprowadzone na ePUAP walidacje zgodności ze wzorami dokumentów.
4.22.	Na czas realizacji projektu Zamawiający zapewni Wykonawcy dostęp do części administracyjnej platformy ePUAP konta Zamawiającego z uprawnieniami do konsoli administracyjnej Draco, ŚBA i usług.
4.23.	W przypadku zwłoki w publikacji wzorów dokumentów CRD realizowanej przez Ministerstwo Cyfryzacji (administrator ePUAP) dopuszcza się dokonanie odbioru tej części zamówienia w ramach lokalnych publikacji w CRD z zastrzeżeniem, że Wykonawca dokona przekonfigurowania aplikacji po pomyślnej publikacji CRD przez Ministerstwo Cyfryzacji.
4.24.	Zamawiający przekaże Wykonawcy opisy usług w formacie MS Word.
4.25.	Zamawiający dopuszcza, aby Wykonawca wykorzystał opisy usług umieszczone na platformie ePUAP.
4.26.	Zadaniem wykonawcy jest odpowiednie powiązanie opisów usług zamieszczonych na ePUAP z odpowiednimi usługami opracowanymi przez Zamawiającego.
4.27.	Wykonawca przygotuje definicję brakujących opisów usług na ePUAP. Zamawiający zwróci się do Ministerstwa Cyfryzacji w celu akceptacji i umieszczenia ich na platformie ePUAP.
4.28.	Wszystkie opisy usług zostaną przyporządkowane do jednego lub więcej zdarzenia życiowego z Klasyfikacji Zdarzeń, a także do Klasyfikacji Przedmiotowej Usług ePUAP.

Zadaniem Wykonawcy jest dostarczenie formularzy, wg. poniższego zapotrzebowania. O ile prawo centralne lub lokalnej nie wymaga inaczej.

Tabela 2 Lista formularzy elektronicznych

Lp.	Rodzaj dokumentu: W- wniosek, Z- zgłoszenie	Nazwa
1.	W	
2.	W	
3.	W	
4.	W	
5.	W	
6.	Z	
7.	W	
8.	Z	
9.	W	
10.	W	
11.	W	
12.	W	
13.	W	
14.	W	
15.	W	
16.	W	
17.	W	
18.	W	
19.	W	

Zakres 6 - Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym oprogramowaniem (m.in.: EOD, Portalu eUsług)

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu używania Systemu na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia, a w szczególności z procedurą migracji danych.

Tabela 3 Minimalny zakres szkoleń

Nr.	Wymaganie
6.1.	Zrealizowanie szkoleń w zakresie obsługi i zarządzania systemami: Elektronicznego Obiegu Dokumentów (zwanego dalej EOD), portalem e-Usług oraz każdym innym oprogramowaniem niestandardowym dostarczanym w ramach postępowania - jeśli wykonawca dostarczy inne oprogramowanie niestandardowe - dla pracowników Zamawiającego w ramach projektu. Szczegółowy zakres poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiający w ramach akceptacji harmonogramu i materiałów szkoleniowych.
6.2.	Szkolenia z systemu EOD przeprowadzone zostaną w według następującego schematu: a) szkolenia grupy kierowników referatów urzędu, wskazanych przez Zamawiającego; b) szkolenia dla grup pracowniczych w max 10 osobowych grupach z merytorycznym udziałem przeszkolonych kierowników; c) szkolenia stanowiskowe pracowników dla min. 30 osób
6.3.	Schematy szkoleń (w tym, m.in.: terminy, ilości godzin, wymagany zakres, ilość osób) z innych systemów (EOD, portalu e-Usług, systemu integrującego, itp.) zostaną ustalone z Wykonawcą indywidualnie po podpisaniu umowy i zapoznaniu się przez Zamawiającego z warunkami minimalnymi w zakresie szkoleń dla każdego z dostarczanych systemów.
6.4.	Do każdego modułu wspomagającego obsługę obszarów działalności urzędu, Zamawiający wskaże osoby, które Wykonawca przeszkoli.
6.5.	Szkolenia zostaną przeprowadzone w sposób możliwie jak najbardziej praktyczny przy wykorzystaniu testowej instancji dostarczanego systemu EOD na sprzęcie zapewnionym przez Wykonawcę lub na komputerach wskazanych przez Zamawiającego. Poszczególne zagadnienia zostaną omówione przez Wykonawcę w zakresie teorii i specyfiki a następnie zaprezentowane w sposób praktyczny. Każde zagadnienie zostanie podsumowane możliwością zadawania dodatkowych pytań uzupełniających przez uczestników szkolenia i stosowanymi wyjaśnieniami

	Wykonawcy, wyczerpującymi dane zagadnienie.
6.6.	Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych.
6.7.	Zamawiający dopuszcza przeprowadzanie szkoleń „indywidualnych" przy stanowiskowych dla grup max. trzyosobowych
6.8.	Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiający w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.
6.9.	Wykonawca zapewni przeszkolenie administratorów wskazanych przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu bazodanowego. Szkolenie musi obejmować co najmniej instalację, konfigurację bazy danych, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.
6.10.	Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie dostarczane systemy oferują i pozwalać pracownikom na rozpoczęcie pracy w systemach.
6.11.	1) Wykonawca zapewni: a) rekrutację uczestników szkoleń spośród pracowników urzędu zapewniając im możliwość wyboru terminu szkolenia, b) zorganizowanie zajęć dostosowanych do poziomu wiedzy uczestników, tak aby każda z grup szkoleniowych wypracowała czas zajęć szkoleniowych. c) pracę uczestników kursu w EOD, d) materiały szkoleniowe niezbędne do nauki teoretycznej i praktycznej treści szkolenia, e) zapoznanie uczestników przed rozpoczęciem szkolenia z programem szkolenia oraz przekazania im harmonogramu realizowanych zajęć, f) organizację szkoleń grup pracowniczych w dni robocze w godzinach pracy, jednorazowe zajęcia trwające około 7 godz. zegarowych (z dwoma przerwami), g) przygotowanie i prowadzenie odpowiedniej dokumentacji, w tym: i) list obecności z podpisami uczestników szkolenia, ii) wystawienie uczestnikom szkolenia dyplomów / zaświadczeń ukończenia szkolenia oraz zebranie pisemnych oświadczeń uczestników potwierdzających ich odbiór, iii) stosowanie na wszystkich dokumentach (materiałach szkoleniowych, programach i harmonogramach szkolenia, listach obecności, dziennikach zajęć, zaświadczeniach itp.) oznaczenia o współfinansowaniu szkolenia z Europejskiego Funduszu Rozwoju Regionalnego, Regionalnego Programu Operacyjnego Województwa Warmińsko Mazurskiego na lata 2014-2020-

	wg obowiązującego wzoru, iv) przekazanie Zamawiającemu w terminie 7 dni od dnia zakończenia szkoleń, następujących dokumentów: (1) oryginałów list obecności, (2) oryginału oświadczenia uczestników potwierdzających odbiór dyplomów (zaświadczeń) ukończenia szkolenia (3) kserokopii dyplomów (zaświadczeń) o ukończeniu szkolenia, (4) oryginału sprawozdania ze zrealizowanych szkoleń.
6.12.	Zakres tematyczny szkoleń musi obejmować: 1. *Rodzaje współczesnej dokumentacji* a. *Dokument elektroniczny* b. *Kategoryzacja dokumentacji tworzonej, napływającej i składanej w podmiocie* c. *Dokumentacja tworząca akta spraw i nie tworząca akta spraw* d. *Rodzaje przesyłek wpływających do podmiotu* e. *przesyłki przekazane pocztą elektroniczną* f. *przesyłki na nośniku papierowym* g. *przesyłki przekazane na informatycznym nośniku danych* h. *przesyłki przekazane na elektroniczną skrzynkę podawczą ePUAP* 2. *Podstawowy system dokumentowania przebiegu, załatwiania i rozstrzygania - System Elektronicznego Zarządzania Dokumentacją (EOD)* a. *Pojęcia i ważne terminy* b. *Akty wewnętrzne dotyczące sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw* c. *Koordynator czynności kancelaryjnych - zadania w EOD* d. *Interoperacyjność znaku sprawy* e. *Akta sprawy w EOD* f. *Metryka sprawy w EOD* 3. *Czynności kancelaryjne w systemie EOD* a. *Zadania punktów kancelaryjnych* i) *otwieranie przesyłek wpływających - wyjątki* ii) *rejestracja wpływów (naklejanie identyfikatora) - wyjątki* iii) *Odwzorowanie cyfrowe (skanowanie) - wyjątki* iv) *wprowadzanie metadanych* v) *tworzenie i prowadzenie składu chronologicznego w podziale na pełne odwzorowanie i niepełne odwzorowanie* vi) *prowadzenie składu informatycznych nośników danych* vii) *wypożyczanie i wycofywanie dokumentacji ze składu chronologicznego i składu informatycznych nośników danych* viii) *przekazywanie do archiwum zakładowego dokumentacji ze składu chronologicznego i składu informatycznych nośników danych*

	ix) wysyłka pisma papierowego i elektronicznego *b. Zadania kierowników komórek organizacyjnych* *i) dekretacja pisma - wyjątki* *ii) dekretacja zastępcza* *iii) akceptacja projektów pism (jedno lub wielostopniowa)* *iv) podpisanie pisma podpisem elektronicznym* *v) podpisanie pisma podpisem odręcznym* *c. Zadania prowadzących sprawy* *i) zakładanie spraw* *ii) uzupełnianie metadanych* *iii) prowadzenie kompletnych akt sprawy* *iv) prowadzenie metryk spraw* *v) sporządzanie projektów pism* *vi) dokonywanie akceptacji,* *4. Korespondencja wewnętrzna w EOD* *a. udostępnianie pism,* *b. przekazywanie pism,* *5. Postępowanie z dokumentacją w przypadku reorganizacji komórek organizacyjnych w EOD* *6. Archiwizacja akt spraw zakończonych w EOD* *a. Organizacja i zadania archiwum zakładowego (składnicy akt),* *b. Lokal archiwum zakładowego (składnicy akt),* *c. Przejmowanie dokumentacji do archiwum zakładowego (składnicy akt),* *d. Przechowywanie i zabezpieczanie zgromadzonej dokumentacji oraz prowadzenie jej ewidencji,* *e. Przeprowadzanie skontrum dokumentacji w archiwum zakładowym oraz porządkowanie dokumentacji w archiwum zakładowym,* *f. Udostępnianie dokumentacji przechowywanej w archiwum zakładowym (składnicy akt),* *g. Wycofywanie dokumentacji ze stanu archiwum zakładowego (składnicy akt),* *h. Brakowanie dokumentacji niearchiwalnej,* *i. Przekazywanie materiałów archiwalnych do archiwów państwowych,* *j. Sprawozdawczość archiwum zakładowego.*

Zakres 7 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył instrukcję dostępu do systemów i sieci Internet [LAN oraz WLAN] zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów/urządzeń.

Dokumentacja musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści.

Zakres 8 – Gwarancja i wsparcie

Świadczenie usługi gwarancji i wsparcia ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp. Zakres i warunki opisane w Załączniku nr 3 do Umowy.

Wykonawca zobowiązuje się do dostarczania wolnych od wad kolejnych wersji Systemu.

Wykonawca zobowiązuje się do aktualizacji dokumentacji Użytkownika i/lub Administratora.

Wykonawca zobowiązuję się do świadczenia konsultacji dla Administratorów w zakresie niezbędnych zmian w konfiguracji systemów aplikacji portalu e-Usług w całym okresie gwarancji.

Wykonawca zapewni usługę wsparcia użytkowników udostępniając:

- usługę typu helpdesk, udostępnioną pod adresem e-mail, numerem telefonu
- portal typu helpdesk – dostępny on-line w trybie 356/7/24, gdzie będą publikowane m.in. statusy zgłoszeń oraz ich treść i historia korespondencji
- przez niniejszy portal będą mogły być dokonywane zgłoszenia Dysfunkcji

Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy systemu zgodnego z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Administratorów związane z bieżącą eksploatacją Systemu.

Wykonawca zapewni w godzinach pracy Zamawiającego w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów.

Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.

Wykonawca będzie świadczył na rzecz Zamawiającego usługi serwisu w zakresie przedmiotu zamówienia (umowy) w okresie wskazanym w ofercie (licząc od daty podpisania protokołu odbioru) zapewniając jednocześnie odpowiednie wsparcie merytoryczne.

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

- z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: Dysfunkcji w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
- związanych z realizacją usługi wdrożenia Systemu;
- spowodowanych aktualizacjami Systemu.

Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów.

Zgłaszający, w przypadku wystąpienia dysfunkcji przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia Dysfunkcji. W Zgłoszeniu powinny być wypełnione wszystkie obligatoryjne pola formularza, a opis sytuacji prowadzącej do wystąpienia błędu lub

awarii powinien umożliwiać jej odtworzenie przez zespół serwisowy Wykonawcy. Jeżeli odtworzenie błędu nie będzie możliwe w środowisku Wykonawcy, wówczas zdiagnozuje on błąd w środowisku Zamawiającego, a terminy usunięcia Dysfunkcji ulegają wydłużeniu o czas oczekiwania na dostęp do środowiska Zamawiającego.

Wykonawca zobowiązany jest do potwierdzenia w ciągu 4 godzin przyjęcie Zgłoszenia oraz jego klasyfikację. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.

Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie.

Zgłoszenia będą klasyfikowane zgodne ze słownikiem pojęć, zawartym w Załączniku nr 3 do Umowy, przez Zamawiającego w uzgodnieniu z Wykonawcą.

Wykonawca zobowiązany jest do usunięcia dysfunkcji w terminach wymienionych w pkt 7 procedury podejmowania prac serwisowych zawartej w Załączniku nr 3 do Umowy.

W każdym przypadku Zgłaszający i Wykonawca mogą uzgodnić inny czas dostarczenia rozwiązania niż określono w warunkach gwarancji. W takim przypadku niezbędne jest potwierdzenie ustalonego terminu w formie pisemnej, faksem lub e-mailem.

Terminy wymienione w Załączniku nr 3 do Umowy obowiązują również w przypadku dostarczonego sprzętu.