Załącznik nr 1 do SIWZ

[SŁOWNIKI I SKRÓTY 2](#_Toc451430858)

[CEL ZAMÓWIENIA 5](#_Toc451430859)

[Wprowadzenie: 5](#_Toc451430860)

[Opis przedmiotu zamówienia : 6](#_Toc451430861)

[Serwer poczty elektronicznej i pracy grupowej. 8](#_Toc451430862)

[System operacyjny na którym będzie działała poczta elektroniczna (POS). 9](#_Toc451430863)

[System lub systemy anty spamowe i antywirusowe (ASP). 11](#_Toc451430864)

[System umożliwiający centralne i automatyczne dodawanie stopek i opisów do przesyłek poczty elektronicznej (STP). 15](#_Toc451430865)

[Licencje na powyższe systemy wraz z niezbędnymi licencjami typu CAL (LIC). 15](#_Toc451430866)

[Licencje na system operacyjny dla serwerów zaplecza (ZOS): 16](#_Toc451430867)

[Pakiet podstawowy oprogramowania biurowego wraz z licencjami zbiorczymi (OBP) 140 sztuk. 18](#_Toc451430868)

[Pakiet rozszerzony oprogramowania biurowego wraz z licencjami zbiorczymi (OBE) 20 sztuk. 19](#_Toc451430869)

[Wdrożenie systemów w środowisku Zamawiającego wraz z migracją z istniejącego systemu (WDR). 20](#_Toc451430870)

[Warsztaty dwóch administratorów Zamawiającego w zakresie administracji i procedur posługiwania się systemami (SAD) 21](#_Toc451430871)

[Szkolenie pracowników Zamawiającego w zakresie posługiwania się systemami (SPR): 21](#_Toc451430872)

[ŚWIADCZENIE USŁUGI SERWISU I GWARANCJI 22](#_Toc451430873)

[WYMAGANIA W ZAKRESIE DOKUMENTACJI 24](#_Toc451430874)

[WYMAGANIA W ZAKRESIE DOSTĘPNOŚCI 28](#_Toc451430875)

[WYMAGANIA W ZAKRESIE ZGODNOŚCI Z PRZEPISAMI PRAWA 29](#_Toc451430876)

#

# SŁOWNIKI I SKRÓTY

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

| Skrót/pojęcie | Definicja |
| --- | --- |
| Awaria | Oznacza sytuację uniemożliwiająca użytkownikom prawidłowe lub pełne korzystanie z Oprogramowania, wadę lub usterkę Oprogramowania, usługi. |
| Błąd  | Oznacza Błąd Krytyczny i/lub Błąd Niekrytyczny i/lub Błąd Zwykły; |
| Błąd Krytyczny | Oznacza brak działania środowiska produkcyjnego Systemu, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Błędy Krytyczne mają jedną lub więcej z poniższych cech: dane biznesowe zostały uszkodzone;Funkcjonalność Krytyczna udokumentowana w Projekcie Technicznym Uzupełnień nie działa;System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji;wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na:uwierzytelnianie,niezaprzeczalność,poufność,integralność,dostępność,rozliczalność,wszelkie błędy związane z bezpieczeństwem dostępu do Systemu (w tym nieautoryzowanym dostępem do danych); |
| Błąd Niekrytyczny | Utrudnia działanie Systemu w środowisku produkcyjnym w zakresie Funkcjonalności Krytycznej i uniemożliwia działanie Systemu w zakresie pozostałych funkcjonalności. W tym kontekście „utrudnia” oznacza istnienie sposobu jego obejścia, stosując przygotowane przez Wykonawcę procedury tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji, (co może mieć wpływ na wygodę w użytkowaniu Systemu lub wymagać procedur ręcznych). „Uniemożliwia” oznacza brak możliwości jego obejścia; |
| Błąd Zwykły | Wszelki błąd niebędący Błędem Krytycznym lub Błędem Niekrytycznym; |
| Dni Robocze | Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8.15 do 16.15; |
| Dokumentacja  | Wytworzone przez Wykonawcę w ramach realizacji Umowy i podlegające zatwierdzeniu przez Zamawiającego materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności Projekt Techniczny, Plan Wdrożenia, Plan Testów Akceptacyjnych (PTA), Dokumentacja Eksploatacyjna, Opis Integracji z Systemem Kopii Bezpieczeństwa, Dokumentacja Powdrożeniowa Systemu , dokumentacja powstała w wyniku realizacji wymagań odbioru produktów, dokumentacja powstała w wyniku realizacji wymagań zarządzania projektem, dokumenty robocze wytworzone przez Wykonawcę w ramach realizacji Umowy; za Dokumentację uznaje się także wytworzenie i aktualizację Dokumentacji w ramach modyfikacji i Nadzoru Autorskiego oraz w okresie gwarancji i świadczenia usług serwisu gwarancyjnego; |
| Funkcjonalności Krytyczne | Cechy funkcjonalne środowiska produkcyjnego:Świadczenie usług poczty elektronicznej, systemu anty – spam i anty –wirus oraz integracji z istniejącym systemem kopii bezpieczeństwa. |
| Incydent serwisowy | Oznacza zgłoszenie do Wykonawcy przez Zamawiającego lub osoby wskazane przez Zamawiającego, w trybie 24 godziny na dobę 7 dni w tygodniu, nieprawidłowości w działaniu Systemu. Wykonawca zobowiązany jest do rejestracji zgłoszenia oraz usuwania Błędów i usterek lub dostarczenia procedur obejścia, powodujących przywrócenie działania Systemu i rozwiązania zgłoszenia.  |
| Lokalizacja | Oznacza pomieszczenie w siedzibie Zamawiającego, do którego Wykonawca dostarczy Oprogramowanie wraz z odnoszącą się dokumentacją techniczną producenta będące przedmiotem niniejszego zamówienia; |
| Nadzór Autorski | Czynności Wykonawcy wykonywane w ramach Zleceń polegające na doradztwie i konsultacjach technicznych, Modyfikacjach oraz pracach związanych z rozbudową, zmianami, usprawnieniami oraz zmianą konfiguracyjną Systemu, oraz dokonywanie zmian Dokumentacji, zgodnie z oczekiwaniami Zamawiającego lub Użytkowników wraz z przeniesieniem w ramach wynagrodzenia za poszczególne Zlecenia majątkowych praw autorskich oraz praw zależnych do zmienionej Dokumentacji; |
| Oprogramowanie Standardowe | Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci.  |
| Plan Testów Akceptacyjnych /PTA | Dokument opracowany przez Wykonawcę podlegający akceptacji Zamawiającego; |
| Projekt Techniczny  | Projekt Techniczny, element Dokumentacji opisujący sposób wykonania, wdrożenia i właściwości Systemu. Szczegółowe wymagania dla Projektu Technicznego zostały określone w wymaganiu DOK.1.1; |
| SLA | Service Level Agreement, poziom dostępności usług |
| System | Infrastruktura sprzętowo - programowa, powstała w wyniku realizacji Umowy.  |
| System Kopii Bezpieczeństwa / SKB | Urządzenia i Oprogramowanie Zamawiającego służące kopiowaniu na nośniki zewnętrzne danych (w szczególności: pliki, bazy danych, rejestry, konfiguracje) gromadzonych na infrastrukturze serwerowej w ramach niniejszego przedmiotu zamówienia. |
| Umowa | Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia; |
| Usługa Serwisu | Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Systemu oraz jego poszczególnych komponentów, w szczególności usuwanie Błędów; |
| Wykonawca/Dostawca | Podmiot realizujący zamówienie; |
| Zamawiający | Centrum Projektów Polska Cyfrowa |
| Zlecenie | Oznacza zamówienie złożone przez Zmawiającego będące podstawą realizacji przez Wykonawcę serwisu i Nadzoru Autorskiego, w tym modyfikacji oraz Szkoleń; |

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem

# CEL ZAMÓWIENIA

Zadanie polega na migracji istniejącego systemu poczty i pracy grupowej wraz z oprogramowaniem wspomagającym do nowocześniejszego środowiska , ujednolicenie oprogramowania pracującego na stacjach roboczych oraz dostarczenie Centrum Projektów Polska Cyfrowa oprogramowania do systemów operacyjnych zaplecza. Postępowanie obejmuje migrację lub rozbudowę obecnych zasobów określonych w tabeli 1 w środowisku klastra określonego w tabeli 2.

## Wprowadzenie:

Obecne środowisko zlokalizowane jest w biurze przy ulicy Syreny 23 w Warszawie, składa się z następujących elementów istotnych dla zamówienia:

Tabela 1 Obecne systemy

|  |  |  |
| --- | --- | --- |
| **Maszyna / System** | **System operacyjny / Inny** | **Usługi** |
| Wirtualna maszyna VMware | Windows 2008 Standard | poczta (Mdaemon) – IMAP , POP3 SMTP |
| Macierz Dell MD 3800f wraz z dodatkową półką na dyski | N/D | Fragment środowiska klastra VMware |
| Fizyczne stacje robocze | Linia MS Windows 7 PRO , Windows 10 PRO | Stacje robocze z oprogramowaniem MS Outlook |
| ArcServe Backup r16.5 (UDP) | Windows 2012 R2 | Agent dla : ARCserve Open Files for Windows , ARCserve for Microsoft Exchange for Windows,ARCserve Guest Based Virtual Machines Bundle |

Tabela 2 Parametry klastra HA Vmware

| **Nazwa zasobu** | **Parametr**  |
| --- | --- |
| vSphere HA | Aktywne |
| Całkowite zasoby CPU | 86Ghz |
| Całkowita ilość pamięci | 383,64 GB |
| Całkowita przestrzeń dyskowa | 15 TB |
| Liczba hostów | 3 |
| Całkowita liczba procesorów | 36 |
| Liczba datastorów | 6 |

Zamawiający dysponuje łączem internetowym o właściwych parametrach oraz certyfikatem ssl typu „wildcard” , wystawionym przez rozpoznawalną organizację .

# Opis przedmiotu zamówienia :

Przedmiotem zamówienia są:

1. Serwer poczty elektronicznej i pracy grupowej .
2. System operacyjny na którym będzie działała poczta elektroniczna.
3. System lub systemy filtrujące spam i przeciwdziałające wniknięciu i rozprzestrzenianiu się wirusów poprzez system.
4. System umożliwiający centralne i automatyczne dodawanie stopek i opisów do przesyłek poczty elektronicznej.
5. Licencje na powyższe systemy wraz z niezbędnymi licencjami typu CAL.
6. Licencje na system operacyjny dla 5 serwerów zaplecza.
7. Pakiet podstawowy oprogramowania biurowego wraz z licencjami zbiorczymi.
8. Pakiet rozszerzony oprogramowania biurowego wraz z licencjami zbiorczymi.
9. Wdrożenie systemów wymienionych w punktach 1 ,2,3 4,5 w środowisku Zamawiającego wraz z migracją z istniejącego systemu.
10. Integracja systemów wymienionych w punktach 1,2,3,4 z systemem kopii bezpieczeństwa Zamawiającego (SKB)
11. Warsztaty dla administratorów Zamawiającego w zakresie administracji i procedur posługiwania się systemami.
12. Szkolenie pracowników Zamawiającego w zakresie posługiwania się systemami.
13. Utrzymanie linii serwisu gwarancyjnego i Nadzoru Autorskiego dla systemu.

Realizacja i zakres

| **Etapy** | **Przedmiot zamówienia** | **Maksymalny czas wyznaczony do realizacji Etapu** |
| --- | --- | --- |
| **Etap 1** | 1. opracowanie i dostarczenie Zamawiającemu Dokumentacji Etapu 1, w szczególności:
2. Projektu Technicznego,
3. Planu Wdrożenia
4. Planu Testów Akceptacyjnych
5. przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu 1 wraz z prawem zezwalania na wykonywanie praw zależnych, na zasadach określonych w istotnych postanowieniach umowy;
6. Dostawa Oprogramowania Standardowego;
 | **7 dni** **od dnia podpisania Umowy** |
| **Etap 2** | 1. instalację, konfigurację, migrację i uruchomienie zgodnie z Projektem Technicznym oraz Planem Wdrożenia odebranego przez Zamawiającego Oprogramowania;
2. przeprowadzenie testów akceptacyjnych Systemu, zgodnie z zatwierdzonym przez Zamawiającego Planem Testów Akceptacyjnych;
 | **18 od dnia** **podpisania Umowy**, |
| **Etap 3** | 1. opracowanie i dostarczenie Zamawiającemu Dokumentacji Etapu 3, w szczególności:

a) Dokumentacji Eksploatacyjnej, b) Opisu Integracji z Systemem z Kopii Bezpieczeństwa;b) Dokumentacji Powdrożeniowej Systemu;1. przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu 3 wraz z prawem zezwalania na wykonywanie praw zależnych, na zasadach określonych w istotnych postanowieniach umowy;
 | **25 od dnia** **podpisania Umowy**, |
| **Nadzór Autorski** | 1. świadczenie Nadzoru Autorskiego w wysokości 100 roboczogodzin, gdzie roboczogodzina oznacza 60 minut, w okresie 24 miesięcy od podpisania protokołu odbioru Etapu 3.
 | **W okresie 24 miesięcy od podpisania Protokołu Odbioru Etapu 3 lub do wcześniejszego wyczerpania przyjętego limitu roboczogodzin** |
| **Warsztaty** | 1. przeprowadzanie przez Wykonawcę warsztatów, w zakresie administrowania Systemu dla 2 osób, realizowanych na podstawie Zleceń;
 | **od dnia podpisania protokołu odbioru Etapu 2 do upływu 30 dni od podpisania protokołu odbioru Etapu** |
| **Szkolenie pracowników** | 1. przeprowadzanie przez Wykonawcę szkolenia pracowników Zamawiającego, w zakresie posługiwania się Systemem;
 | **60 dni od dnia podpisania protokołu odbioru Etapu 2**  |
| **Gwarancja** | 1. udzielenie gwarancji i świadczenie usługi serwisu gwarancyjnego dla Systemu w okresie 12 miesięcy od podpisania protokołu odbioru Etapu 2, oraz na prace wykonane w ramach Nadzoru Autorskiego, w tym Modyfikacje, od dnia podpisania danego Protokołu Odbioru Zlecenia na podstawie, którego prace te są odbierane do upływu 24 miesięcy od dnia podpisania Protokołu Odbioru Etapu 3;
 | **Gwarancja na Oprogramowanie i konfigurację dostarczone w ramach Etapu 1 biegnie od dnia podpisania Protokołu Odbioru Etapu 2, w okresie 12 miesięcy od podpisania protokołu odbioru Etapu 2, oraz na prace wykonane w ramach Nadzoru Autorskiego, w tym Modyfikacje, od dnia podpisania danego Protokołu Odbioru Zlecenia na podstawie, którego prace te są odbierane do upływu 24 miesięcy od dnia podpisania Protokołu Odbioru Etapu 3** |

Szczegółowe warunki stawiane dla zamawianych składników :

### Serwer poczty elektronicznej i pracy grupowej.

#### Skalowanie systemu poczty (SPE):

Na dzień zakończenia wdrożenia system musi obsługiwać 180 skrzynek pocztowych o średnim rozmiarze 8 GB , przy szacowanym przepływie poczty do 2000 przesyłek dziennie.

System musi być skalowalny do 300 - 500 użytkowników i rozmiar łączny skrzynek (baz) do 4 TB , przy czym skalowanie musi polegać na rozszerzeniu ilości licencji dostępowych i zmianach sprzętowych w zakresie przestrzeni do składowania baz.

Wymagania

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| SPE.01 | Prawidłowy przepływ poczty elektronicznej wewnątrz jak i na zewnątrz organizacji. |
| SPE.02 | Szyfrowanie dla poczty buforowanej na stacjonarnych i przenośnych urządzeniach klasy PC. |
| SPE.03 | Dostęp do poczty elektronicznej, kalendarza i kontaktów niezależnie od lokalizacji przy użyciu komputerów stacjonarnych i przenośnych oraz urządzeń mobilnych z wykorzystaniem protokołów *https*, *RPC over https* , *OMA* i *Active-Sync*. |
| SPE.04 | Centralne składowanie poczty elektronicznej w tym kontaktów i kalendarzy w organizacji w strukturze jednorodnej bazy danych. |
| SPE.05 | Możliwość śledzenia przepływu poczty elektronicznej w ramach organizacji. |
| SPE.06 | Mechanizm delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania. |
| SPE.07 | Mechanizm detekcji zajętości kalendarza i urlopów typu „Free/Busy” |
| SPE.08 | Integracje z rozwiązaniem katalogowym opartym na *AD*. |
| SPE.09 | Intuicyjny , przejrzysty i prosty interfejs administracyjny. |
| SPE.10 | Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań bez przyznawania pełnych uprawnień administracyjnych. |
| SPE.11 | Możliwość wykonywania kopii bezpieczeństwa systemu umożliwiającej odzyskanie pojedynczej wiadomości z pojedynczej skrzynki. |
| SPE.12 | Protokoły automatycznej konfiguracji klientów poczty. |
| SPE.13 | Planowanie spotkań w obrębie organizacji przy zachowaniu zdolności wysyłania zaproszeń i zdarzeń zgodnych z normą RFC 2445 poza organizacje. |
| SPE.14 | Udostępniania kalendarzy do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu |
| SPE.15 | Tworzenia centralnych archiwów poczty , zawierających elementy przenoszone do tychże na podstawie centralnie obowiązujących polis , przy zachowaniu zgodności z procedurami dotyczącymi materiałów dowodowych. |
| SPE.16 | Centralne tworzenie reguł przechowywania. |
| SPE.17 | Tworzenia grup dystrybucyjnych , w tym grup o moderowanym uczestnictwie. |
| SPE.18 | Tworzenia aliasów adresów poczty elektronicznej. |
| SPE.19 | Tworzenia skrzynek recepcyjnych , nadawania uprawnień do wysyłania „W imieniu”. |
| SPE.20 | Tworzenia obiektów ( skrzynek pocztowych ) dla infrastruktury , służących planowaniu wykorzystania zasobów („*Room - Resource Mailbox*”). |
| SPE.21 | Włączania i wyłączania protokołów obsługi poczty zarówno dla organizacji jak i poszczególnych użytkowników. |
| SPE.22 | Wprowadzenia ograniczenia wielkości skrzynki pocztowej i przesyłki zarówno w kontekście pojedynczego użytkownika jak i organizacji. |
| SPE.23 | Utworzenia klastra typu „*Load-balance*” lub „*Fail-over*” z bliźniaczym rozwiązaniem przy pomocy technologii *DAG* , *LCR* , *CCR* lub zbliżonej . |
| SPE.24 | Umożliwić integrację z cyfrowym systemem telefonicznym i usługami „*Voice mail form*„ , „*Play on Phone*” i „*Outlook Voice Access*” |
| SPE.25 | Posiadać zorganizowany przez producenta system szkoleń i materiałów edukacyjnych w języku polskim. |

### **System operacyjny na którym będzie działała poczta elektroniczna (POS).**

Wymagania:

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| POS.01 | Zalecany przez producenta systemu poczty  |
| POS.02 | Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  |
| POS.03 | Możliwość budowania klastrów. |
| POS.04 | Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  |
| POS.05 | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  |
| POS.06 | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  |
| POS.07 | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  |
| POS.08 | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  |
| POS.09 | Wbudowane wsparcie instalacji i pracy na wolumenach, które: 1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
3. pozwalają na zmianę rozmiaru w czasie pracy systemu,
4. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
5. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
6. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 |
| POS.10 | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  |
| POS.11 | Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  |
| POS.12 | Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  |
| POS.13 | Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  |
| POS.14 | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  |
| POS.15 | Dostępne dwa rodzaje graficznego interfejsu użytkownika - klasyczny i dotykowy.  |
| POS.16 | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  |
| POS.17 | Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  |
| POS.18 | Mechanizmy logowania w oparciu o login i hasło, karty z certyfikatami (smartcard), wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  |
| POS.19 | Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników.  |
| POS.20 | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  |
| POS.21 | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  |
| POS.22 | Zapewnić dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  |
| POS.23 | Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  |
| POS.24 | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 |
| POS.25 | Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 |
| POS.26 | Zdalna dystrybucja oprogramowania na stacje robocze.  |
| POS.27 | Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  |
| POS.28 | Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1. Dystrybucję certyfikatów poprzez http
2. Konsolidację CA dla wielu lasów domeny,
3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 |
| POS.29 | Szyfrowanie plików i folderów.  |
| POS.30 | Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  |
| POS.31 | Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  |
| POS.32 | Serwis udostępniania stron WWW.  |
| POS.33 | Wsparcie dla protokołu IP w wersji 6 (IPv6),  |
| POS.34 | Wsparcie dla algorytmów Suite B (RFC 4869),  |
| POS.35 | Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  |
| POS.36 | Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.  |
| POS.37 | Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  |
| POS.38 | Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  |
| POS.39 | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  |
| POS.40 | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  |
| POS.41 | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  |
| POS.42 | Zorganizowany przez producenta system szkoleń i materiałów edukacyjnych w języku polskim. |

### System lub systemy anty spamowe i antywirusowe (ASP).

#### Właściwości i funkcjonalności

Mechanizm ochrony antyspamowej musi zapewniać możliwość tworzenia polityk ochrony antyspamowej, w szczególności z uwzględnieniem:

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| ASP.01 | Licencja na środowisko wirtualne VMware ESXi/ESX/vSphere 4.x, 5.x lub Microsoft Hyper-V 2008/2012. |
| ASP.02 | Integracja z LDAP: Active Directory (zarówno LDAP jak i Global Catalog), iPlanet Directory/Sun Directory Server 6.x/7.0, Lotus Domino LDAP Server 7.0/8.x, OpenLDAP 2.x |
| ASP.03 | Zintegrowane rozwiązanie antywirusowe, antyspamowe i filtrowania treści. |
| ASP.04 | Praca, jako bramka pocztowa. |
| ASP.05 | Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowana na serwer usługodawcy. |
| ASP.06 | Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 98%. Równocześnie rozwiązanie ma charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, potwierdzonym przez niezależne testy. |
| ASP.07 | Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów. |
| ASP.08 | System ma zapewnić routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy. |
| ASP.09 | System ma mieć możliwość zmiany domeny i nazwy użytkownika w wiadomości przychodzącej i wychodzącej dla odbiorcy i nadawcy odpowiednio dla ruchu przychodzącego i wychodzącego. |
| ASP.10 | System ma umożliwiać tworzenie aliasów dla grup użytkowników. |
| ASP.11 | System ma zapewnić dopisywanie domyślnej nazwy domeny dla nadawcy wiadomości. |
| ASP.12 | System ma zapewnić ochronę przed skanowaniem serwera pocztowego w poszukiwaniu istniejących (prawidłowych) adresów pocztowych. |
| ASP.12 | Usuwanie nagłówków Received z wysyłanych wiadomości. |
| ASP.13 | Wiadomości z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu). |
| ASP.14 | Wiadomości z systemów próbujących atakować wirusami serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako wirusy z jednego IP w danym przedziale czasu). |
| ASP.15 | Połączenia z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu). |
| ASP.16 | Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie się zawsze odbywać. |
| ASP.17 | Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana. |
| ASP.18 | Niezależnie konfigurowane polityki dla wiadomości przychodzących i wychodzących, |
| ASP.19 | Funkcja ograniczająca dostępne pasmo dla maszyn/domen przesyłających spam, ale nieblokująca w całości komunikacji z tymi maszynami/domenami. |
| ASP.20 | Aktualizacje sygnatur spamu nie rzadziej, niż co 1 min. |
| ASP.21 | Aktualizacje sygnatur antywirusowych nie rzadziej, niż co 1 godzina. |
| ASP.22 | Rozwiązanie antywirusowy ma skanować skompresowane załączniki do 10 poziomów zagnieżdżeń w głąb i ma być odporna na złośliwie spreparowane załączniki („załączniki bomby”). |
| ASP.23 | Wiadomości z wirusami typu mass-mailer mają być w całości odrzucane, bez podejmowania dodatkowych akcji takich jak np. powiadomienie. |
| ASP.24 | Wykrywanie fałszywych URL-i w wiadomościach. |
| ASP.25 | Wykorzystanie technologii znakowania załączników dla odróżnienia ich treści. |
| ASP.26 | Wykorzystanie technologii analizy html mających na celu przeciwdziałanie metodom utrudniającym analizę treści wiadomości (np.: losowo generowane ciągi, nieprawidłowe kody formatujące). |
| ASP.27 | Detekcja języka, w którym została napisana wiadomość i możliwość użycia tej informacji, jako kryterium przy przetwarzaniu wiadomości. |
| ASP.28 | Kontrola treści w oparciu o słowa kluczowe lub słowniki definiowana przez administratora, w tym sprawdzanie zawartości skompresowanych archiwów. |
| ASP.29 | Zaawansowane mechanizmy tworzenia reguł kontroli treści, wiązanie wymagań przy pomocy logicznych I i LUB, możliwość budowanie reguł w postaci negatywnej NIE. |
| ASP.30 | Możliwość dodawania do wysyłanych wiadomości zdefiniowanego tekstu. |
| ASP.31 | Nakładanie polityk na załączniki w oparciu o ich rozmiar, typ MIME, nazwa pliku lub jego rozszerzenie – w tym identyfikację prawdziwego rozszerzenia pliku. |
| ASP.32 | Wiadomości sklasyfikowane, jako spam można:1. Usunąć.
2. Dodać nagłówek wiadomości.
3. Zmodyfikować – dodać informację dla odbiorcy.
4. Zarchiwizować.
5. BCC – wysłać blind carbon copy na inny adres pocztowy.
6. Bounce – odpowiedzieć nadawcy wiadomością z modyfikowalnym NDR.
7. Wyczyścić, jeśli wiadomość zawierała wirusa.
8. Dostarczyć bez modyfikacji.
9. Przekierować na inny adres pocztowy.
10. Zmodyfikować temat wiadomości.
11. Wrzucić wiadomość do centralnej kwarantanny.
12. Przesłać powiadomienie na wybrany adres.
13. Usunąć załącznik z wiadomości.
 |
| ASP.33 | Możliwość wysłania wiadomości spam niewykrytych przez rozwiązanie do producenta, w celu ich analizy. |
| ASP.34 | Rozróżnienie kategorii wiadomości na: 1. Normalne wiadomości bez spamu i wirusów.
2. Spam.
3. Podejrzane o spam.
4. Biuletyn (tzw. newsletter).
5. Wiadomość marketingowa.
6. Wiadomość z podejrzanym adresem URL.
7. Wirusy masowe.
8. Wiadomości zawierające wirusy.
9. Wiadomości, których nie można przeskanować.
10. Wiadomości od blokowanych nadawców.
11. Wiadomości zablokowane na podstawie filtrów przygotowanych przez administratora.
 |
| ASP.35 | Wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID. |
| ASP.36 | Import bazy użytkowników poprzez LDAP. |
| ASP.37 | Administrator ma mieć możliwość ingerencji w czułości rozwiązania. |
| ASP.38 | Rozwiązanie ma posiadać serwer kwarantanny. Serwer ma być dostępny dla poszczególnych użytkowników końcowych. Serwer ma przesyłać okresowe powiadomienia o zawartości kwarantanny. Powiadomienia mają mieć wbudowane mechanizmy do zarządzania zawartością kwarantanny (przesłanie dalej, podgląd, zalogowanie do kwarantanny). |
| ASP.39 | Na serwer kwarantanny można nałożyć ograniczenia dla poszczególnych użytkowników jak i całego serwera wg ilości przechowywanych wiadomości, ilości zajętego miejsca. |
| ASP.41 | Użytkownik końcowy rozwiązania ma mieć możliwość definiowania własnych list blokowanych i przepuszczanych nadawców wiadomości, ingerencje w zachowanie systemu detekcji języka i możliwość wysłania do producenta systemu źle sklasyfikowanych wiadomości. |
| ASP.42 | Komunikacja pobierania uaktualnień ma być szyfrowana.  |
| ASP.43 | Komunikacja w celu zarządzania systemem ma być szyfrowana. |
| ASP.44 | Rozwiązanie ma być centralnie zarządzane z wbudowanymi mechanizmami raportowania. Jedna konsola ma umożliwić zarządzania kilkoma współpracującymi urządzeniami. Wykonywane raporty mają uwzględniać dane zebrane ze wszystkich współpracujących urządzeń. |
| ASP.45 | System ma posiadać przynajmniej 55 wbudowanych raportów. Wykonanie raportów można zaplanować w dzienniku. Gotowe raporty można przesłać do skrzynki pocztowej wyznaczonych odbiorców. |
| ASP.46 | System ma umożliwiać tworzenie wielu kont administracyjnych z różnymi poziomami uprawnień, w tym możliwość zdefiniowania użytkowników mających dostęp do różnych kwarantann. |
| ASP.47 | System ma umożliwiać definiowanie poziomu logowania o swojej aktywności. |
| ASP.48 | System ma powiadamiać wybranych administratorów o nieprawidłowej pracy komponentów. |
| ASP.49 | System ma umożliwiać wykonywanie zaplanowanych kopii bezpieczeństwa konfiguracji i baz kwarantanny oraz możliwość odtworzenia konfiguracji z tak wykonanej kopii. |
| ASP.50 | Ograniczony zestaw poleceń dostępny z konsoli systemu operacyjnego. |
| ASP.51 | System ma umożliwiać graficzne śledzenie wiadomości, w tym informacje, co stało się z wiadomością. |
| ASP.52 | System ma posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych. |
| ASP.53 | System ma umożliwiać zapytanie o adres IP do wewnętrznej i globalnej bazy reputacji. |
| ASP.54 | System ma umożliwiać stworzenie odpowiednio obsługiwanych kolejek z punktu widzenie reputacji danego adresu IP – ograniczając taki adres do ilości wysyłanych wiadomości, ilości nawiązywanych połączeń w określonym czasie. |
| ASP.55 | System ma mieć możliwość zdefiniowania osobnej kwarantanny dla poczty naruszającej reguły zgodności z polityką określającą rodzaj przesyłanych treści. |
| ASP.56 | System musi umożliwiać skorzystania z predefiniowanych polityk i wzorców. |
| ASP.57 | System ma umożliwiać rozpatrywanie incydentów skojarzonych z naruszeniem polityk, w tym definiowanie ważności incydentu. |
| ASP.58 | Rozpatrując incydent muszą być z góry określone akcje, które osoba rozpatrująca incydent może podjąć, np. rozpoczęcie śledztwa, przesłanie widomości do odbiorcy, przesłanie wiadomości do nadawcy, itp. |
| ASP.59 | System ma posiadać ochronę przed atakami wirusów typu Day Zero, oraz zdefiniowaną kwarantannę dla złapanych w ten sposób wirusów z możliwością ustawienia czasu, przez który zatrzymane maile mają w niej pozostawać. |
| ASP.60 | System musi umożliwiać wysyłkę źle sklasyfikowanych wiadomości typu spam do producenta, gdzie automatycznie zostaną przygotowane sygnatury antyspamowe i natychmiast dostarczone do rozwiązania. |
| ASP.61 | System ma dodatkowo posiadać możliwość wysyłania alertów SNMP. |
| ASP.62 | System ma umożliwiać integrację z UPS-em. |
| ASP.63 | System musi wspierać autentykację DomainKeys Identified Mail (DKIM). |
| ASP.64 | System musi wspierać autentykację SMTP. |
| ASP.65 | System musi wykorzystywać Bounce Attack Tag Validation (BATV). |
| ASP.66 | System musi zapewniać dedykowaną ochronę dla potencjalnie niebezpiecznej zawartości (makra, skrypty, osadzony Flash, itp.) znajdującej się w plikach PDF oraz plikach pakietu Microsoft Office, polegającą na przebudowaniu takiego dokumentu, usuwając z niego potencjalnie niebezpieczną zawartość według określonego kryterium – np.: usuwaj Flash, pozostaw makra. |
| ASP.67 | Subskrybcja definicji spamu i wirusów lub systemu , o ile taka występuje musi być ważna przez okres 36 miesięcy od daty zakupu. |

### System umożliwiający centralne i automatyczne dodawanie stopek i opisów do przesyłek poczty elektronicznej (STP).

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| STP.01 | Zapewnia automatyczne dodawanie stopek email i noty prawnej na serwerze poczty |
| STP.02 | System jest zarządzany centralnie. |
| STP.03 | Stopka jest budowana automatycznie w oparciu o definiowane reguły z wykorzystaniem przynależności wysyłającego do grup lub kontenerów AD. |
| STP.04 | System umożliwia osadzenie grafiki i zdjęć w formacie in-line w podpisach email.  |
| STP.05 | System pobiera atrybuty z katalogu AD i umieszcza je w podpisach. |
| STP.06 | Posiada wsparcie dla zaszyfrowanych i podpisanych cyfrowo wiadomości. |
| STP.07 | Posiada możliwość dołączenia zdjęcia w podpisach pobieranego z Active Directory.  |
| STP.08 | Zapewnia wyświetlanie stopek w Elementach Wysłanych w tym na urządzeniach mobilnych. |
| STP.09 | Posiada wbudowany edytor szablonów stopek do formatów HTML, RTF i plain text. |
| STP.10 | Umożliwia generowanie kodów QR w podpisach. |
| STP.11 | Umożliwia wdrożenie filtrowania przesyłek zgodnie z polityką Data Loss Protection. |
| STP.12 | Umożliwia usuwanie motywów i papeterii Outlook |
| STP.13 | Umożliwia modyfikowanie formatu wiadomości ( HTML ,RTF, PLAIN)  |

### Licencje na powyższe systemy wraz z niezbędnymi licencjami typu CAL (LIC).

Wymagania

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| LIC.01 | Licencje mają umożliwić jednoczesny dostęp do systemu ( zarówno poczty jak i systemu operacyjnego na którym jest poczta zainstalowana ) dla 180 użytkowników (*User-CAL*) zgodnie z polityką licencjonowania producenta. |
| LIC.02 | Licencja mają być dostarczane drogą elektroniczną. |
| LIC.03 | Model licencjonowania umożliwiający użycie wersji wcześniejszych pakietu na podstawie tej samej licencji. |
| LIC.04 | Licencje mają być typu „Licencji dla jednostek publicznych” , o ile producent oprogramowania wspiera taki typ. |

### Licencje na system operacyjny dla serwerów zaplecza (ZOS):

Wymagania

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| ZOS.01 | Zalecany przez producenta systemu poczty |
| ZOS.02 | Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. |
| ZOS.03 | Możliwość budowania klastrów. |
| ZOS.04 | Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |
| ZOS.05 | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |
| ZOS.06 | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |
| ZOS.07 | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
| ZOS.08 | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. |
| ZOS.09 | Wbudowane wsparcie instalacji i pracy na wolumenach, które:1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
3. pozwalają na zmianę rozmiaru w czasie pracy systemu,
4. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
5. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
6. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 |
| ZOS.10 | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |
| ZOS.11 | Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |
| ZOS.12 | Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET |
| ZOS.13 | Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. |
| ZOS.14 | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. |
| ZOS.15 | Dostępne dwa rodzaje graficznego interfejsu użytkownika - klasyczny i dotykowy. |
| ZOS.16 | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, |
| ZOS.17 | Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. |
| ZOS.18 | Mechanizmy logowania w oparciu o login i hasło, karty z certyfikatami (smartcard), wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), |
| ZOS.19 | Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników. |
| ZOS.20 | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
| ZOS.21 | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
| ZOS.22 | Zapewnić dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
| ZOS.23 | Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |
| ZOS.24 | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 |
| ZOS.25 | Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
 |
| ZOS.26 | Zdalna dystrybucja oprogramowania na stacje robocze. |
| ZOS.27 | Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej |
| ZOS.28 | Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:1. Dystrybucję certyfikatów poprzez http
2. Konsolidację CA dla wielu lasów domeny,
3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 |
| ZOS.29 | Szyfrowanie plików i folderów. |
| ZOS.30 | Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). |
| ZOS.31 | Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. |
| ZOS.32 | Serwis udostępniania stron WWW. |
| ZOS.33 | Wsparcie dla protokołu IP w wersji 6 (IPv6), |
| ZOS.34 | Wsparcie dla algorytmów Suite B (RFC 4869), |
| ZOS.35 | Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, |
| ZOS.36 | Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. |
| ZOS.37 | Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
| ZOS.38 | Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). |
| ZOS.39 | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |
| ZOS.40 | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
| ZOS.41 | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| ZOS.42 | Zorganizowany przez producenta system szkoleń i materiałów edukacyjnych w języku polskim. |

### Pakiet podstawowy oprogramowania biurowego wraz z licencjami zbiorczymi (OBP) 140 sztuk.

Wymagania

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| OBP.01 | Zawiera arkusz kalkulacyjny umożliwiający dokonywanie obliczeń zestawionych w formie tabelarycznej i posiadający funkcje matematyczne, finansowe i bazodanowe. Powinien również wspierać co najmniej półautomatyczne powielanie tworzonych formuł z zastosowaniem różnych wariantów adresowania (adresowanie względne, adresowanie bezwzględne, adresowanie mieszane) jak i obsługę raportów z użyciem tabel przestawnych. |
| OBP.02 | Zawiera edytor tekstu *WYSIWYG* zapisujący dane w formacie *OOXML ,* z możliwością obsługi makr napisanych w języku *VBA.* |
| OBP.03 | Zawiera klienta poczty elektronicznej z obsługą protokołu *MAPI* i *CDO* . Program powinien zawierać również obsługę kalendarza, list z kontaktami oraz innych informacji osobistych i zespołowych. Konieczna jest możliwość tworzenia zabezpieczonych (szyfrowanych ) zbiorów przechowywania powyższych informacji. |
| OBP.04 | Zawiera program do tworzenia prezentacji multimedialnych , umożliwiający zapis prezentacji w formacie Windows Media Video \*.wmv |
| OBP.05 | Posiada lokalizację językową na Polskę. |
| OBP.06 | Posiada zorganizowany przez producenta system szkoleń i materiałów edukacyjnych dostępny w języku polskim. |
| OBP.07 | Posiada komercyjny system wsparcia użytkownika realizowany przez producenta bądź jego oficjalnych przedstawicieli. |
| OBP.08 | Posiada model licencjonowania umożliwiający uruchamianie poszczególnych aplikacji w trybie aplikacji terminalowych (RDC). |
| OBP.09 | Model licencjonowania umożliwiający użycie wersji wcześniejszych pakietu na podstawie tej samej licencji. |
| OBP.10 | Licencje dostarczone mają być typu „Licencji dla jednostek publicznych”. |
| OBP.11 | Pracuje na systemie rodziny MS Windows 7 i wzwyż , ze wsparciem dla architektury 64 bity. |

### Pakiet rozszerzony oprogramowania biurowego wraz z licencjami zbiorczymi (OBE) 20 sztuk.

Wymagania

| **Kod wymagania** | **Opis wymagania** |
| --- | --- |
| OBP.01 | Zawiera arkusz kalkulacyjny umożliwiający dokonywanie obliczeń zestawionych w formie tabelarycznej i posiadający funkcje matematyczne, finansowe i bazodanowe. Powinien również wspierać co najmniej półautomatyczne powielanie tworzonych formuł z zastosowaniem różnych wariantów adresowania (adresowanie względne, adresowanie bezwzględne, adresowanie mieszane) jak i obsługę raportów z użyciem tabel przestawnych. |
| OBP.02 | Zawiera edytor tekstu *WYSIWYG* zapisujący dane w formacie *OOXML ,* z możliwością obsługi makr napisanych w języku *VBA.* |
| OBP.03 | Zawiera klienta poczty elektronicznej z obsługą protokołu *MAPI* i *CDO* . Program powinien zawierać również obsługę kalendarza, list z kontaktami oraz innych informacji osobistych i zespołowych. Konieczna jest możliwość tworzenia zabezpieczonych (szyfrowanych ) zbiorów przechowywania powyższych informacji. |
| OBP.04 | Zawiera program do tworzenia prezentacji multimedialnych , umożliwiający zapis prezentacji w formacie Windows Media Video \*.wmv |
| OBP.05 | Zawiera system lub program do obsługi relacyjnych baz danych, z własnym , wbudowanym silnikiem bazy danych, służący zarówno do obsługi jak i szybkiego prototypowania aplikacji bazodanowych. |
| OBP.06 | Zawiera program do tworzenia materiałów marketingowych, przeznaczonych do druku (DTP) pozwalającym na ich drukowanie, zamieszczanie w sieci Web. |
| OBP.07 | Posiada lokalizację językową na Polskę. |
| OBP.08 | Posiada zorganizowany przez producenta system szkoleń i materiałów edukacyjnych dostępny w języku polskim. |
| OBP.9 | Posiada komercyjny system wsparcia użytkownika realizowany przez producenta bądź jego oficjalnych przedstawicieli. |
| OBP.10 | Posiada model licencjonowania umożliwiający uruchamianie poszczególnych aplikacji w trybie aplikacji terminalowych (RDC). |
| OBP.11 | Model licencjonowania umożliwiający użycie wersji wcześniejszych pakietu na podstawie tej samej licencji. |
| OBP.12 | Licencje dostarczone mają być typu „Licencji dla jednostek publicznych”. |
| OBP.13 | Pracuje na systemie rodziny MS Windows 7 i wzwyż , ze wsparciem dla architektury 64 bity. |

### Wdrożenie systemów w środowisku Zamawiającego wraz z migracją z istniejącego systemu (WDR).

Wymagania minimalne

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDR.01 | Konfiguracja wirtualnych maszyn i zasobów na potrzeby systemu pocztowego i systemów anty spam , antywirus i automatyki stopki w środowisku Zamawiającego. |
| WDR.02 | Asysta przy konfiguracji protokołów sieciowych i usług niezbędnych do prawidłowego działania systemu na urządzeniach zamawiającego.  |
| WDR.03 | Instalacja i konfiguracja systemów operacyjnych i oprogramowania systemu pocztowego i systemów anty spam , antywirus i automatyki stopki. |
| WDR.04 | Konfiguracja oprogramowania systemu pocztowego i systemów anty spam , antywirus i automatyki stopki zgodnie z przedłożonym przez Wykonawcę projektem. |
| WDR.05 | Przeprowadzenie Testów Akceptacyjnych. |
| WDR.06 | Migracja użytkowników i usług na nową platformę z zachowaniem następującej funkcjonalności :1. Ciągłość pracy poczty zarówno wewnątrz jak i na zewnątrz organizacji
2. W trakcie migracji poczta przychodząca do organizacji musi dotrzeć do użytkownika niezależnie czy został przeniesiony na nowy system czy funkcjonuje w starym.
3. Poczta wewnątrz organizacji musi dotrzeć do użytkownika niezależnie czy został przeniesiony na nowy system czy funkcjonuje w starym.
4. Obydwa systemy objęte są mechanizmami kontroli spamu i wirusów
5. Opracowany sposób migracji musi zapewnić dostęp użytkownika końcowego do zasobów pochodzących ze starego systemu , takich jak poczta elektroniczna wraz ze struktura folderów , kontakty czy też informacje kalendarzowe.
6. Opracowany sposób musi zapewnić jak największą automatykę procesu migracji.
 |
| WDR.07 | Integracja systemów z istniejącym mechanizmem kopii bezpieczeństwa.  |
| WDR.08 | Archiwizację starego środowiska. |
| WDR.09 | Usunięcie starego środowiska.  |

### Warsztaty dla dwóch administratorów Zamawiającego w zakresie administracji i procedur posługiwania się systemami (SAD)

Wymagania

|  |  |
| --- | --- |
| **Kod Wymagania** | **Zakres wymagania** |
| SPR.01 | Warsztaty wewnętrzne z zakresu procedur administracji i konserwacji uwzględnionych w dokumentacji DOK.1.4  |
| SPR.02 | Ekwiwalent bieżącego kursu MS o numerze 20342 (lub następca) , dla oferowanej technologii - zaawansowane rozwiązania systemu pocztowego i pracy grupowej realizowane przez autoryzowany ośrodek szkoleniowy Producenta. |
| SPR.03 | Ekwiwalent bieżącego kursu MS o numerze 20341 (lub następca), dla oferowanej technologii - podstawowe zagadnienia systemu pocztowego i pracy grupowej realizowane przez autoryzowany ośrodek szkoleniowy Producenta. |
| SPR.07 | Szkolenia zakończą się egzaminem przeprowadzonym w ośrodku egzaminowania certyfikowanym przez producenta oprogramowania. |

### Szkolenie pracowników Zamawiającego w zakresie posługiwania się systemami (SPR):

#### Wymagania i zakres :

Wykonawca przeprowadzi w siedzibie Zamawiającego 6 dwugodzinnych szkoleń zrealizowanych w terminie 2 dni roboczych w zakresie wdrażanego klienta pocztowego zgodnie z przedstawionym zakresem dla użytkowników Zamawiającego zgodnie z przedstawionym zakresem:

|  |  |
| --- | --- |
| **Kod Wymagania** | **Zakres wymagania** |
| SPR.01 | Klient poczty i pracy grupowej – wygląd i foldery1. Opis interfejsu.
2. Foldery i widoki.
 |
| SPR.02 | Praca z wiadomościami elektronicznymi.1. Wysyłanie, odbieranie, odpowiadanie, przekazywanie.
2. Funkcja UDW.
3. Odwoływanie i zamienianie wiadomości wysłanych.
4. Śledzenie wiadomości e-mail za pomocą potwierdzeń przeczytania.
 |
| SPR.03 | Zarządzanie folderami i wiadomościami w folderach.1. Wyszukiwanie wiadomości.
2. Delegacja uprawnień.
 |
| SPR.04 | Kontakty. 1. Tworzenie kontaktów osobistych.
2. Przesyłanie kontaktów.
3. Praca z globalną książką adresową.
 |
| SPR.05 | Praca z kalendarzem.1. Zarządzanie spotkaniami, terminami, wydarzeniami cyklicznymi.
2. Zrządzanie czasem wolnym, lokalizacją spotkań.
3. Praca grupowa, żądanie i udzielanie uprawnień.
 |
| SPR.06 | Zadania.1. Zlecanie, wykonywanie zadań.
2. Kontrola wykonywanych zadań .
 |
| SPR.07 | Inne.1. Funkcja auto-konfiguracji.
2. Skrzynki współdzielone.
3. Reguły.
4. Współpraca z urządzeniami mobilnymi
 |

# ŚWIADCZENIE USŁUGI SERWISU I GWARANCJI

| **Kod wymagania** | **Opis funkcjonalności** |
| --- | --- |
| WUS.1 | Wykonawca będzie przyjmował zgłoszenia o Incydentach serwisowych w trybie **24 godziny na dobę 7 dni** **w tygodniu**. |
| WUS.2 | W celu zarządzania Incydentami serwisowymi Wykonawca zapewni system do obsługi Incydentów serwisowych, za pomocą, którego dokonywane będą zgłoszenia Incydentów serwisowych, obsługa i monitorowanie Incydentów serwisowych (np. system oparty na komunikacji za pomocą poczty elektronicznej ze zgłaszającym Incydent serwisowy lub zakładający interakcję ze zgłaszającym Incydent serwisowy, za pomocą graficznego interfejsu użytkownika lub stanowiący połączenie obydwu ww. form). |
| WUS.2.1 | Wykonawca umożliwi przyjęcie i obsługę Incydentów serwisowych kierowanych faksem lub mailem na adres podany przez Wykonawcę. |
| WUS.3 | Usunięcie Błędu zostanie zakończone przywróceniem działania Oprogramowania sprzed Błędu. |
| WUS.4 | Wykonawca najpóźniej w 1 Dzień Roboczy, po rozwiązaniu Incydentu serwisowego przedstawi raport z tego Incydentu serwisowego (prezentujący, co najmniej czasy przyjęcia zgłoszenia o Incydencie serwisowym oraz rozwiązania Incydentu serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Incydentu serwisowego). |
| WUS.7 | W przypadku zgłoszeń serwisowych niemieszczących się w zakresie świadczonych usług wynikających z niniejszego zamówienia, Wykonawca zobowiązany jest do przekierowania zgłoszenia serwisowego do odpowiedniego podmiotu na zasadach określonych przez Zamawiającego.  |
| WUS.8 | Gwarancja na dostarczone Oprogramowanie biegnie osobno dla każdego z oprogramowania, od dnia podpisania Protokołu Odbioru Oprogramowania dostarczonych Zamawiającemu w ramach Etapu 1, zaś od dnia podpisania Protokołu Odbioru Etapu 2 – w pozostałym zakresie, przez okres 12 miesięcy od podpisania protokołu odbioru Etapu 2.  |
| WUS.9 | Wykonawca dokona usunięcia Błędu Niekrytycznego w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia Błędu Niekrytycznego (usunięcie Błędu Niekrytycznego rozumiane jest, jako przywrócenie funkcjonalności Systemu sprzed Błędu Niekrytycznego). |
| WUS.10 | Wykonawca dokona usunięcia Błędu Zwykłego w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia Błędu Zwykłego (usunięcie Błędu Zwykłego rozumiane jest, jako przywrócenie funkcjonalności Systemu sprzed Błędu Zwykłego). |
| WUS.13 | Przez usunięcie Błędów rozumie się rozwiązanie problemu albo zaproponowanie procedury obejścia zaistniałych Błędów bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę. |
| WUS.15 | Gwarancja obejmuje również wykonanie przez Wykonawcę wszelkich czynności związanych z przywróceniem pierwotnego stanu pracy Systemu (sprzed Błędu) . |
| WUS.16 | W okresie udzielenia gwarancji na Oprogramowanie Standardowe Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania Standardowego do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware), patch’y, programów korekcji wszelkich błędów (w szczególności Błędów Krytycznych, Błędów Zwykłych, Błędów), a także dostęp do usług wsparcia technicznego producenta danego Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu wymagane informacje umożliwiające Zamawiającemu dostęp do usług wsparcia technicznego producenta oraz aktualizacji w okresie gwarancji, a także każdorazowo w przypadku zmian informacji przekazanych Zamawiającemu.Zamawiający wymaga od Wykonawcy realizacji w ramach Umowy, w tym w okresie gwarancji, prac związanych z dostosowaniem i przetestowaniem Systemu do przedmiotowych aktualizacji Oprogramowania Standardowego (włączając tzw. firmware). |
| WUS.17 | Zamawiający zastrzega sobie prawo do dodawania nowych modułów dowolnych producentów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Oprogramowania, bez utraty gwarancji na zakupione Oprogramowanie. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. |
| WUS.18 | Gwarancja obejmuje między innymi:* + wady materiałowe i konstrukcyjne, a także nie spełnienie deklarowanych przez producenta parametrów i/lub funkcji Oprogramowania i jego konfiguracji;
	+ naprawę wykrytych uszkodzeń;
	+ usuwanie wykrytych usterek i Błędów w działaniu Oprogramowania lub jego konfiguracji.
 |
| WUS.19 | Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie Systemu. |
| WUS.20 | Wsparciem od strony Wykonawcy dla Oprogramowania będzie zajmowała się osoba posiadająca ważny stosowny certyfikat producenta na poziomie odpowiadającym certyfikacji Microsoft nr 70-341 lub 70-342 dla oferowanego systemu. |

# WYMAGANIA W ZAKRESIE DOKUMENTACJI

Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy dokumentację spełniającą wymagania określone w poniższej tabeli.

**- minimalne wymagania dla Dokumentacji.**

| Kod wymagania | Opis funkcjonalności |
| --- | --- |
| DOK.1 | Zamawiający wymaga, aby Wykonawca przygotował, zgodnie z ogólnie akceptowalnymi standardami w dziedzinie dokumentowania, następujące rodzaje Dokumentacji bezpośrednio związanej z przedmiotem zamówienia: |
| DOK.1.1 | W ramach Projektu Technicznego Wykonawca opracuje i dostarczy następujące dokumenty:* Opracowanie architektury rozwiązania (zawierający w szczególności model instalacji komponentów systemu i ich wzajemnych interakcji wraz z ich specyfikacją i zapotrzebowaniem na zasoby).
* Szczegółowy opis realizacji wymagań,
* Szczegółowy wykaz Oprogramowania (zawierający m.in. producenta, nazwę produktu, wykaz komponentów produktu, typ produktu, typ licencji, ilość licencji, listę polskich dystrybutorów produktu),
* Zapisy licencyjne Oprogramowania Standardowego,
 |
| DOK.1.1.1 | Opis integracji z Systemu Kopii Bezpieczeństwa - Wykonawca opracuje i dostarczy dokument zawierający opis procedur wykorzystanych do integracji tworzonego Systemu z istniejącym systemem kopii bezpieczeństwa Zamawiającego . Dokument zawierać będzie: * informacje odnośnie Urządzeń oraz Oprogramowania wykorzystanego do wykonania integracji Systemu.
* Opis konfiguracji utworzonej na potrzeby tego rozwiązania.
 |
| DOK.1.1.2 | Plan wdrożenia systemu – Wykonawca opracuje i dostarczy dokument zawierający szczegółowy opis procedur wykorzystanych do migracji istniejącego środowiska zamawiającego do tworzonego systemu |
| DOK.1.1.3 | Plan Testów Akceptacyjnych (PTA) - dokument PTA musi być przygotowany przez Wykonawcę  |
| DOK.1.2 | Dokumentację Eksploatacyjną**,** zawierającą, co najmniej procedury: administracyjne, backupu systemu i danych, awaryjne i użytkownika, przy czym każda z procedur musi zawierać, co najmniej następujące wyszczególnione informacje:* procedury związane z administracją i eksploatacją,
* procedury o charakterze testowym,
* procedury działania administratora dla wdrożonego Systemów,
* procedury konserwacji dla funkcjonalności integrującej wdrożony System z istniejącym Systemem Kopii Bezpieczeństwa,
* procedury awaryjne,
* procedury kontroli bezpieczeństwa Systemu (Audyt),
* procedura identyfikacji i kwalifikacji Błędu,
* procedury kwalifikacji zgłoszeń serwisowych,
* procedury eskalacji zgłoszeń serwisowych.
* Każda z ww. procedur będzie zawierać minimum następujące informacje:
	+ identyfikator i nazwa procedury,
	+ rodzaj procedury,
	+ data utworzenia i zatwierdzenia oraz wersja procedury,
	+ cel i zakres procedury,
	+ uzasadnienie zastosowania,
	+ warunki uruchomienia procedury i oczekiwany oraz możliwy rezultat jej wykonania,
	+ dane osób, które opracowały procedurę, sprawdziły, zaakceptowały i zatwierdziły,
	+ wzór formularza zgłoszenia Błędu (dla procedur awaryjnych),
	+ szczegółowy opis rezultatów,
	+ możliwe niepowodzenia,
	+ przebiegi alternatywne,
	+ algorytm działania, jaki należy zastosować, wykonując kolejne czynności, aby osiągnąć postawiony cel, w tym z informacją o osobie, która powinna wykonać dane czynności.

Procedury muszą zostać zoptymalizowane pod kątem ciągłości działania usług o maksymalnie wysokim poziomie SLA. |
| DOK.2 | Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak:* Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób.
* Zachowanie standardów, w tym notacji UML, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu.
* Zachowanie standardów Zamawiającego w zakresie oznaczeń dokumentów wersjonowania, metryk.
* Kompletność dokumentu rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia.
* Spójność i niesprzeczność dokumentu rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
 |
| DOK.3 | Cała Dokumentacja, podlega akceptacji Zamawiającego i zostanie dostarczona w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie MS Word i niezabezpieczonym formacie PDF (na płycie CD/DVD lub innym równoważnym nośniku danych) i drukowanej, co najmniej w 1 egzemplarzu (dopuszcza się inne formaty zapisu dokumentacji np. diagramy UML lub formaty wektorowe jak DWG, DXF, należy jednak dołączyć przeglądarkę obsługującą wykorzystane formaty). Diagramy UML sporządzone za pomocą narzędzi CASE muszą być dostarczone w formacie EAP. Dostarczone wykresy Gantta muszą być dostarczone w formacie MPP lub w formacie XLS umożliwiającym import do MS Project.  |
| DOK.3.1 | Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu pliki źródłowe zastosowanych w niej obrazów, w tym m.in. schematów, rysunków, topologii oraz wykresów, w formacie niezabezpieczonym i edytowalnym.  |
| DOK.3.2 | Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu wszystkie dokumenty robocze wytworzone w takcie realizacji niniejszego zamówienia, w szczególności analizy, arkusze kalkulacyjne, materiały robocze, w formacie elektronicznym, niezabezpieczonym i edytowalnym. |
| DOK.3.3 | Wszystkie Dokumenty przekazane w formie elektronicznej (pliki) muszą:* być posegregowane w folderach zgodnie ze strukturą Dokumentacji,
* posiadać nazwy plików (razem ze ścieżką) krótsze niż 200 znaków,
 |
| DOK.3.4 | W przypadku kolejnych wersji Dokumentacji wymagane jest, aby Wykonawca dostarczał elektroniczne wersje Dokumentacji, które zawierają wyróżnione różnice pomiędzy kolejnymi wersjami Dokumentacji (w trybie rejestracji zmian).  |
| DOK.4 | Wykonawca w Etapie 3 Umowy dostarczy Zamawiającemu Wykaz Ilościowo-Cenowy przedmiotu zamówienia z podziałem dla każdego Etapu:1. dokumentów – wykazanie co najmniej Projektu Technicznego, Dokumentacji Powdrożeniowej , Dokumentacji Eksploatacyjnej,
2. oprogramowania – wykazanie każdego Oprogramowania,
3. usług – wykazanie co najmniej prac instalatorsko-konfiguracyjnych dla Oprogramowania, warsztatów,
4. wartości niematerialne i prawne – wykazanie licencji Oprogramowania Standardowego i autorskich praw majątkowych do Dokumentacji wytworzonych w Etapie 1 i 3.

W zakresie co najmniej:* + - nazwa,
		- producent,
		- kod produktu
		- opis,
		- ilość,
		- Lokalizacja instalacji,
		- cena jednostkowa brutto w PLN,
		- cena jednostkowa netto w PLN,
		- wartość brutto w PLN.
 |
| DOK.5 | Wykonawca przedstawi do akceptacji Zamawiającego dokument ‘Dokumentacja Powdrożeniowa Systemu, zawierający co najmniej:* Wprowadzenie opisujące cele i zakres przedmiotu zamówienia,
* Diagram kontekstowy zaproponowanego rozwiązania i model zachowania,
* Ograniczenia rozwiązania, założenia i zależności
* Opis wymagań funkcjonalnych i poza funkcjonalnych Systemu,
* Opis rozwiązania wydajności, skalowalności i niezawodności przebiegu testów akceptacyjnych i sposób oszacowania niezawodności zaproponowanego rozwiązania, w tym propozycję raportów z testów,
* Przebieg (wraz ze szczegółowym opisem) prac i czynności wdrożeniowych (w tym napotkanych problemów wraz z opisem ich rozwiązania),
* Szczegółowy opis działania wytworzonych w ramach niniejszego Zamówienia procedur (w tym napotkanych problemów jako przebiegi alternatywne wraz z opisem ich rozwiązania),
* Szczegółowy opis procedur (wraz z zalecanym harmonogramem) które należy wykonywać w celu prawidłowego utrzymania Systemu,
 |
| DOK.6 | Wykonawca do Dokumentacji dostarczanej w ramach etapu 1 i 3 dołączy wykaz zawierający szczegółowy spis Dokumentów wraz z opisem ich przeznaczenia. |

# WYMAGANIA W ZAKRESIE DOSTĘPNOŚCI

Minimalne wymagania w zakresie dostępności.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDSYS.1 | Zapewnienie architektury rozwiązania gwarantującej niezawodność Systemu napoziomie SLA ustalonym w Umowie, nie mniej niż 99% (niedostępność w skalimiesiąca 7.2 godz.).SLA liczone jest, jako suma czasu trwania niedostępności Systemuspowodowanego Błędami Krytycznymi, przy czym okna serwisowe związanez konserwacją/rekonfiguracją Systemu nie podlegają uwzględnianiu w obliczeniuSLA (termin i zakres prac realizowanych w ramach okna serwisowego wymagauzyskania przez Wykonawcę uprzedniej akceptacji Zamawiającego). |

**WYMAGANIA W ZAKRESIE ZGODNOŚCI Z PRZEPISAMI PRAWA**

Minimalne wymagania w zakresie zgodności z przepisami prawa.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| PR.1 | Rozwiązanie dla Systemu musi być zgodne z niżej wymienionymi aktami prawnym:* Ustawa o ochronie danych osobowych z dnia 29.08.1997 roku. (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926 z późn. Zm.);
* Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12.04.2012 r. (Dz. U. z 2012 r., poz. 526);
* Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17.02.2005 roku (tekst jednolity Dz. U. z 2013 r., poz. 235 z późn. zm.);

Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (tekst jednolity Dz. U. z 2014 r., poz. 243); |