Numer postępowania:

ZP/p/32/2023

**Załącznik nr 3 do SWZ**

# Opis Przedmiotu Zamówienia

**Zakup sprzętu i oprogramowania do środowiska odtworzenia kopii zapasowych oraz rozwój systemu poczty elektronicznej wraz z systemem bezpieczeństwa**

1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest:

# Dostawa sprzętu i oprogramowania na potrzeby budowy środowiska do monitorowania i testowania kopii zapasowych systemów HIS/ERP;

# Rozwój systemu poczty elektronicznej wraz z systemem bezpieczeństwa obejmującym mechanizmy SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową.

1. **Termin realizacji zamówienia oraz liczba dostarczanego sprzęt**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Przedmiot dostawy** | **Liczba dostarczanego Sprzętu/ Oprogramowania** | **Termin dostawy Sprzętu/Oprogramowania** |
| **1** | **Serwer plików wraz z dyskami (NAS) i oprogramowaniem** | **1** | **Do 14 dni kalendarzowych od dnia zawarcia Umowy** |
| **2** | **System poczty elektronicznej Zimbra wraz z systemem bezpieczeństwa**  | **1** | **Do 14 dni kalendarzowych od dnia zawarcia Umowy** |

1. **Szczegółowy Opis przedmiotu zamówienia**
2. **Część I zamówienia – dostawa sprzętu i oprogramowania na potrzeby budowy środowiska do monitorowania i testowania kopii zapasowych systemów HIS/ERP**

Spis przedmiotu zamówienia:

1. Serwer plików wraz z dyskami.
2. Monitoring kopii zapasowych systemów HIS/ERP wraz z usługą odtwarzania i testowania odtworzonych systemów (z 12 miesięczną gwarancją)

# Serwer plików wraz z dyskami.

|  |  |
| --- | --- |
| **Element** | **Opis** |
| **Obudowa** | * Serwer typu RACK, wysokość 2U, dodatkowa półka typu RACK, wysokość 2U
* Szyny umożliwiające zamocowanie serwera oraz półki w szafie stelażowej;
* Możliwość zainstalowania 24 dysków twardych hot plug 3,5”, 12 szt. w serwerze oraz 12 szt. w dodatkowej półce;
 |
| **Płyta główna** | * Dwuprocesorowa;
* Możliwość instalacji procesorów 38-rdzeniowych;
* Możliwość zainstalowania modułu TPM 2.0;
* złącz PCI Express generacji 4 w ilości 7: 4 o prędkości x 16; 3 o prędkości 8, opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości, Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e,
* 32 gniazda pamięci RAM z obsługą minimum 4 TB pamięci RAM DDR4 i 10 TB pamięci w konfiguracji DDR4 + pamięć nieulotna (Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci);
* Wsparcie dla technologii: Memory Scrubbing, SDDC, ECC, Memory Mirroring, ADDDC;
* Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  nie zajmujące klatek dla dysków hot-plug
 |
| **Procesory** | * Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,8 GHz, architektura x86\_64;
* osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 154 pkt  (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie „<http://spec.org/cpu2017/results/cpu2017.html>”
 |
| **Pamięć RAM** | 64 GB pamięci RAM, DDR4 Registered 3200Mhz |
| **Dyski**  | 2 szt. dysków SSD SATA 960GB DWPD>2,5 Hot-Plug;skonfigurowane w RAID podpięte do sprzętowego kontrolera;Zainstalowane 22 szt. dysków Hot-Plug 16TB;Prawo zachowania dysków u Zamawiającego w przypadku ich awarii  |
| **Karty sieciowe** | * Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express,4x 1Gbit Base-T, Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe.;
* Interfejsy LAN zainstalowane w slotach PCI-e: 2x 25Gbit SFP28.
 |
| **Kontrolery I/O** | * Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;
* Kontroler SAS RAID dla dysków w dodatkowej półce posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania.
 |
| **Porty** | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
* 2 porty USB 3.0 wewnętrzne;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* 2 porty USB 3.0 na panelu przednim;
* Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
* Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
 |
| **Zasilanie, chłodzenie** | * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
* Redundantne wentylatory hotplug
 |
| **Zarządzanie** | **Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;*** informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

- karty zainstalowane w dowolnym slocie PCI Express- CPU- Pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM- wbudowany na płycie głównej nośnik pamięci M.2 SSD- status karty zarządzającej serwera,- wentylatory,- bateria podtrzymująca ustawienia BIOS płyty głównej,- zasilacze,- system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym)**Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:*** Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
* Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
* Dostęp poprzez przeglądarkę Web, SSH;
* Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
* Zarządzanie alarmami (zdarzenia poprzez SNMP);
* Możliwość przejęcia konsoli tekstowej;
* Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
* Obsługa serwerów proxy (autentykacja);
* Obsługa VLAN;
* Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
* Wsparcie dla protokołu SSDP;
* Obsługa protokołów TLS 1.2, SSL v3;
* Obsługa protokołu LDAP;
* Integracja z HP SIM;
* Synchronizacja czasu poprzez protokół NTP;
* Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;

**Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);****Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;****Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;****Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.** |
| **Wspierane OS** | * Microsoft Windows Server 2022, 2019, 2016;
* VMWare vSphere 6.7, 7.0;
* Suse Linux Enterprise Server 15;
* Red Hat Enterprise Linux 7.9, 8.3;
* Hyper-V Server 2016, 2019
 |
| **System operacyjny** | Licencja na system operacyjny Microsoft Windows Server Standard 2016 x64 PL/ENG lub równoważny. System operacyjny musi być kompatybilny z dostarczanym serwerem, tj. występować w dokumentacji producenta jako system przeznaczony do dostarczanego serwera. Licencja powinna być odpowiednia do konfiguracji dostarczanego serwera. |
| **Gwarancja** | * 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).
 |

**Równoważność:**

**Oprogramowanie typu MS Windows Server Standard 2016 64bit lub równoważne, spełniające poniższe minimalne wymagania:**

1. Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012.
2. Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), Windows Management Instrumentation.
3. Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji.

**Dokumentacja, Zgodność ze standardami**

* Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
* Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
* Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwera. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.
* Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
* Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

# Monitoring kopii zapasowych systemów HIS/ERP wraz z usługą odtwarzania i testowania odtworzonych systemów (z 12 miesięczną gwarancją)

## 2.1 Monitoring kopii zapasowych systemów HIS/ERP

Konfiguracja środowiska do monitorowania statusów wykonywanych kopii zapasowych krytycznych zasobów infrastruktury IT a w szczególności infrastruktury środowiska HIS i ERP Ma na celu zapobieganie problemom oraz zagrożeniach w wykonaniu kopii zapasowych baz danych i aplikacji, poprzez informowanie administratorów szpitala z odpowiednim zdefiniowanym czasie.

Konfiguracja musi obejmować przygotowanie serwera monitorowania, przygotowanie oraz personalizację szablonów, konfigurację powiadomień, szkolenie z obsługi oraz podpięcie do monitorowania systemu kopii zapasowych środowisk HIS i ERP działających u Zamawiającego.

**Wymagania szczegółowe**

|  |  |
| --- | --- |
| 1 | Umożliwiać monitorowanie statusów wykonania kopii zapasowych wykonywanych co najmniej przez narzędzia:* Veeam
* Veritas
* Bacula
* Bareos
* RMAN (oracle)
 |
| 2 | Umożliwiać, przez definiowanie tzw. pułapek, przyjmowanie informacji (np. statusów) z systemów nie mających interfejsów zewnętrznych (tj. API)  |
| 3 | dodatkowo powinno umożliwiać monitorowanie systemów operacyjnych, urządzeń sieciowych, łączy internetowych, baz danych |
| 4 | obsługiwać co najmniej systemy operacyjne rodziny Windows i Linux |
| 5 | posiadać mechanizmy monitorowania plików logów tekstowych |
| 6 | gromadzić dane w bazie danych i obsługiwać co najmniej MySQL, mariaDB, PostgreSQL,Oracle |
| 7 | posiadać prekompilowanych agentów na systemy rodziny Windows oraz Linux |
| 8 | umożliwiać weryfikację poprawności pracy agentów monitorowania |
| 9 | umożliwiać definiowanie odrębnych parametrów monitorowania oraz wartości progowych dla różnych rodzajów serwerów w zależności od ich konfiguracji i roli. |
| 10 | umożliwiać definiowanie grup serwerów w zależności od ich konfiguracji i roli |
| 11 | gromadzić i utrzymywać informacje historyczne monitorowanych elementów infrastruktury |
| 12 | udostępniać za pośrednictwem interfejsu graficznego informacje o skonsolidowanym stanie serwerów w czasie rzeczywistym. |
| 13 | udostępniać za pośrednictwem interfejsu graficznego informacje o aktualnych listach problemów wymagających reakcji. |
| 14 | powiadamiać administratorów o niedostępności monitorowanych serwerów i urządzeń. |
| 15 | szyfrować komunikację pomiędzy serwerem monitorowania a agentami |
| 16 | mieć możliwość monitoringu zarówno agentowego jak i bezagentowego. |
| 17 | realizować dostęp do systemu monitorowania poprzez konta dla upoważnionych użytkowników i chronić je hasłem |
| 18 | umożliwiać elastyczne definiowanie widoków dla użytkowników w zależności od ich roli, potrzeb oraz uprawnień. |
| 19 |  monitorować wydajność i pojemność zasobów sprzętowych serwerów: a) procesory, b) pamięć operacyjna, c) przestrzenie dyskowe, d) interfejsy sieciowe. |
| 20 | musi umożliwiać wysyłanie powiadomień o zdarzeniach zarówno przez email jak i SMS |
| 21 | musi umożliwiać prezentowanie danych historycznych w postaci wykresów |
| 22 | musi posiadać szablony konfiguracyjne zawierające predefiniowane ustawienia monitorowania |
| 23 | musi automatycznie wyliczać SLA dla wybranych serwisów |
| 24 | musi umożliwiać prezentacje wizualną infrastruktury np. za pomocą map sieci |
| 25 | musi umożliwiać budowania własnych szablonów monitorowania |
| 26 | musi mieć możliwość dynamicznego dodawania elementów do monitorowania (np. dynamicznie budować listę dysków systemu operacyjnego i dodawać do nich parametry do monitorowania) |
| 27 | musi monitorować zadane parametry i na podstawie zadanych granicznych wartości generować odpowiednio ostrzeżenia lub błędy |
| 28 | musi obsługiwać SNMP |
| 29 | musi monitorować usługi systemu HIS i ERP działającego u Zamawiającego |
| 30 | musi monitorować pracę systemu PACS działającego u Zamawiającego |
| 31 | musi monitorować bazy danych, co najmniej Oracle, MySQL, PostgreSQL |
| 32 | musi monitorować działania bramek HL7, działających u Zamawiającego  |
| 33 | musi umożliwiać monitorowanie parametrów wydajnościowych systemu HIS działającego u zamawiającego |
| 34 | musi być możliwość uruchomienia serwera monitorowania jako maszyny wirtualnej |
| 35 | Zmawiający wymaga aby instalacja środowisko było na maszynie wirtualnej |
| 36 | Szkolenia co najmniej dwóch administratorów z dostarczanego rozwiązania. Tak aby administrator finalnie mógł zarządzać i samodzielnie dodać nowe urządzenia lub usługo |
| 37 | dostarczenie dokumentacji powykonawczej |
| 38 | Usługa jest dostarczona na 12 miesiące, więc wykonawca zapewni, iż przez 12 miesięcznej gwarancji będzie usuwał wszystkie wady dostarczonej usługi oraz co najmie wykonał raz na kwartał aktualizacje. |

## 2.2 Usługa odtworzenia systemów HIS/ERP z kopii zapasowych

Usługa polega na odtwarzaniu elementów środowiska HIS/ERP, z posiadanych przez Zamawiającego kopii zapasowych, na dodatkowym, odseparowanym od produkcyjnego, dedykowanym środowisku odtworzeniowym. Wykonywana będzie określoną ilość razy w okresie 12 miesięcy od zamówienia oraz po przekazaniu niezbędnych dostępów do infrastruktury. Realizowana będzie przy użyciu wdrożonych już u Zamawiającego mechanizmów kopii zapasowych, które są tak skonfigurowane, że umożliwiają odtworzenie danych bezpośrednio na środowisku odtworzeniowym. Zamawiający przekaże wymaganą dokumentację środowiska kopii zapasowych, środowiska odtworzeniowego oraz niezbędne dane dostępowe. Po każdym odtworzeniu Wykonawca musi sporządzić raport, który zawierał będzie informacje o przeprowadzonych pracach a w szczególności, z których kopii zostało wykonane odtworzenie, ile czasu trwało odtworzenie oraz które elementy HIS podlegały testowi odtworzenia. Po odtworzeniu Zamawiający dokona weryfikacji środowiska i potwierdzi poprawność prac Wykonawcy.

**Wymagania szczegółowe**

W ramach usługi, Wykonawca po przeprowadzeniu odtworzenia, musi przeprowadzić następujące testy:

1. weryfikacja podłączenia odtworzonych usług do bazy danych systemu HIS
2. logowanie do systemu HIS (EskulapNT, EskulapNG)
3. weryfikacja uprawnień eWUŚ
4. generacja nowego dokumentu EDM
5. podgląd istniejących dokumentów EDM
6. przyjęcie pacjenta do szpitala
7. logowanie do systemu ERP (aplikacja Impuls)
8. logowanie do systemu ERP (Portal Pracowniczy)

Po odtworzeniu zostanie przygotowany raport, który będzie zawierał co najmniej informacje:

1. wykaz elementów podlegających testowi odtworzenia
2. informacje o źródłowych kopiach danych
3. opis zastosowanej procedury/mechanizmu odtworzenia
4. wykaz czasów odtworzenia poszczególnych elementów HIS/ERP
5. wykaz niezbędnych czynności, jakie trzeba wykonać po odtworzeniu w podziale
	1. serwery aplikacyjne
	2. bazy danych

Każdy test odtworzenia, musi zawsze zawierać odtworzenie baz danych systemów HIS i ERP.

1. **Część II zamówienia - rozwój systemu poczty elektronicznej wraz z systemem bezpieczeństwa obejmującym mechanizmy SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową**.

Spis przedmiotu zamówienia:

1. Migracja istniejącego systemu poczty Zimbra Open Source do wersji komercyjnej
2. Wdrożenia zaawansowanego systemu antyspamowego

# Migracja istniejącego systemu poczty Zimbra Open Source do wersji komercyjnej

**Wymagania techniczne system poczty elektronicznej:**

1. Dostarczenie niewygasających licencji systemu dla 800 kont użytkowników z 36 miesięcznym wsparciem technicznym producenta zaoferowanego systemu.
2. Dostarczenie polskojęzycznej dokumentacji użytkownika końcowego w wersji filmów instruktarzowych.
3. Przeprowadzenie szkolenia dla użytkowników kluczowych systemu w siedzibie Zamawiającego.
4. Dostarczenie polskojęzycznej dokumentacji powdrożeniowej.
5. Udzielenie asysty technicznej wdrażającego (Wykonawcy) dostępnej w maksymalnym okresie 36 miesięcy.

Serwer systemu poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

Funkcjonalności podstawowe:

* 1. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
	2. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
	3. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
	4. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
	5. Możliwość tworzenia zadania z wiadomości pocztowej z poziomu klienta w przeglądarce.
	6. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
	7. Obsługa innych aplikacji za pomocą interfejsów SOAP/REST/API poprzez udostępnianie usług (np. Web-services).
	8. Możliwość zablokowania przesłania i przekazywania wiadomości do domen zewnętrznych.
	9. System udostępnia API programistyczne za pomocą którego można integrować się z systemami trzecimi.
1. Możliwość wykorzystania Microsoft Active Directory do uwierzytelniania użytkowników, prezentacji listy użytkowników w globalnej książce adresowej i SSO.
2. Możliwość wykorzystania zewnętrznych katalogów LDAP do uwierzytelniania użytkowników i prezentacji listy użytkowników w globalnej książce adresowej.
3. Możliwość jednoczesnej, bezawaryjnej pracy 800 użytkowników łączących się do serwera za pomocą klienta Web bądź innego oprogramowania opartego o standardowe protokoły IMAP, SMTP, CalDAV.
4. System pocztowy musi być skalowalny do obsługi ponad 1000 kont użytkowników lub więcej, przy wykorzystaniu dodatkowego sprzętu, bez konieczności reinstalacji.
5. System musi być zabezpieczony przed lukami bezpieczeństwa wynikającymi z technologii, w której został stworzony.

Funkcjonalność zaawansowana:

1. Możliwość uzyskania pełnego wsparcia dla klienta poczty elektronicznej MS Outlook 2013 i nowszych wersji oprogramowania MS Outlook od 2013 do 2019, w ramach możliwości zakupu w późniejszym czasie dodatkowych licencji dla środowiska.
2. Możliwość realizacji mechanizmu wymuszenia polityk zabezpieczeń na urządzeniach mobilnych z systemami Android, Windows Phone i iOS. Polityki powinny wymuszać zdefiniowane hasła, czy jego złożoność, czy też możliwość szyfrowania pamięci urządzenia i kart pamięci, w ramach możliwości zakupu w późniejszym czasie dodatkowych licencji dla środowiska.

Funkcjonalności pozostałe:

1. Możliwość drukowania wiadomości oraz wyświetlania podglądu wydruku. Możliwość wyboru i drukowania wielu wiadomości jednocześnie.
2. Możliwość definiowania reguł filtrowania i priorytetów dla wiadomości przychodzących i wychodzących.
3. Możliwość stosowania nowych reguł na istniejących wiadomościach.
4. Możliwość definiowania własnego podpisu. Możliwość konfiguracji przez administratorów maksymalnej liczby znaków używanych w podpisach.
5. Przeciągnięcie wybranej wiadomości do kalendarza powoduje automatyczne utworzenie terminu na podstawie tej wiadomości.
6. Prezentowanie wiadomości poczty elektronicznej użytkownika z poziomu interfejsu webowego w widoku wg kolejności napływania lub grupującym w konwersacje.
7. Możliwość zdefiniowania priorytetu wysyłanej wiadomości pocztowej.
8. Możliwość załączania definiowalnej przez administratora liczby załączników do wysyłanej wiadomości elektronicznej o rozmiarze maksymalnym definiowalnym przez administratora
9. Pobieranie dużej ilości załączników wiadomości elektronicznej w postaci jednej paczki (np. skompresowanego archiwum zip).
10. Wyświetlanie bieżącej zajętości przestrzeni skrzynki użytkownika.
11. Wyszukiwanie wiadomości wg zadanych kryteriów min.: adresu/nazwy nadawcy/odbiorcy, temacie wiadomości, dacie wysłania.
12. Możliwość oznaczenia wiadomości flagą lub znacznikami definiowanymi przez użytkownika umożliwiającymi grupowanie szybsze wyszukiwanie wiadomości.
13. Obsługa funkcjonalności drag&drop w interfejsie webowym w zakresie przenoszenia wiadomości pomiędzy folderami.
14. Interfejs webowy do obsługi poczty powinien współpracować poprawnie z przeglądarkami internetowymi zarówno w systemach stacjonarnych jak i mobilnych
15. Interfejs webowy powinien udostępniać tryb nowoczesny, który jest responsywny i reaktywny, dostosowujący się do urządzenia na którym wyświetlana jest ten interfejs, opierający się o nowoczesne frameworki, np. Preact, React, Vue.js
16. Interfejs webowy do obsługi poczty powinien umożliwić użytkownikowi tworzenie wiadomości przez edytor WYSWIG z możliwością stosowania rożnego rodzaju formatowań, krojów czcionek, styli itp.
17. Umożliwienie użytkownikowi wysyłanie wiadomości w formacie tekstowym lub HTML.
18. Automatyczne podpowiadanie adresu odbiorcy z dostępnych książek adresowych podczas tworzenia wiadomości.
19. Interfejs webowy do obsługi poczty powinien umożliwić użytkownikowi obsługę innych kont pocztowych poprzez protokół POP3 lub IMAP (funkcja nadawana użytkownikowi tylko przez administratora).
20. Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi zdefiniowanie parametrów odpowiedzi automatycznej. Wymagane parametry autorespondera to czas działania, treść odpowiedzi, przekierowanie wiadomości na inny adres, itp.
21. Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi zdefiniowanie przekazywania wiadomości na inny adres poczty elektronicznej np. na czas jego nieobecności w pracy, urlopu. Definiowalne powinno być ograniczenie przesyłania tylko do własnej domeny.
22. Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi ustawienie żądania potwierdzenia odbioru wiadomości przez odbiorcę.
23. Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi zmianę hasła na żądanie oraz wg polityki złożoności zdefiniowanej przez administratora
24. Możliwość zablokowania konta użytkownika po określonej liczbie nieudanych prób logowania w zadanym okresie czasu.
25. Możliwość zdefiniowania podpisu użytkownika dołączanego automatycznie do każdej nowej wysyłanej wiadomości.
26. Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi eksport/import książki adresowej do pliku CSV.
27. Możliwość odzyskania skasowanej przez użytkownika wiadomości z folderu „kosz” z poziomu interfejsu webowego pracy grupowej.
28. Możliwość personalizacji wyglądu interfejsu webowego przez użytkownika poprzez dostępne w systemie pracy grupowej szablony wyglądu i kolorystyki, rodzaje czcionek oraz układy elementów widoku.

Konakty

1. Możliwość prezentacji kontaktów jako listy.
2. Możliwość importu, eksportu kontaktów z, do pliku .CSV, .VCF przez administratora lub użytkownika.
3. Możliwość utworzenia przez użytkownika wielu książek adresowych w ramach jednego konta.
4. Możliwość przenoszenia i kopiowania kontaktów pomiędzy książkami adresowymi (w oparciu o uprawnienia dostępu).
5. Możliwość tworzenia przez użytkowników grup kontaktów.

Kalendarz

1. Możliwość planowania spotkań i podglądu dostępności innych uczestników (wolny, zajęty).
2. Możliwość zmiany przez użytkownika własnej informacji o dostępności.
3. Możliwość tworzenia spotkań cyklicznych oraz wyjątków do spotkań cyklicznych.
4. Możliwość rezerwacji zasobów (lokalizacja, wyposażenie, itp.) w ramach spotkania.
5. Możliwość wyszukiwania dostępnych zasobów poprzez atrybuty (budynek, piętro, itp.).
6. Możliwość włączenia alertu (pop-up) w związku ze zbliżającym się terminem.
7. Możliwość prezentacji kalendarza w widokach: dzień, tydzień, miesiąc, dzień (godziny pracy), tydzień (godziny pracy).
8. Możliwość konfiguracji godzin i dni roboczych.
9. Możliwość tworzenia spotkania we wszystkich widokach kalendarza.
10. Możliwość szybkiego akceptowania lub odrzucania terminu.
11. Możliwość włączenia lub wyłączenia przez użytkownika automatycznych powiadomień e-mail na temat spotkań.
12. Możliwość tworzenia przez użytkownika wielu kalendarzy w ramach jednego konta.
13. Możliwość wyświetlania przez użytkownika wielu kalendarzy nakładanych w tym samym miejscu. Każdy kalendarz reprezentowany jest przez inny kolor.
14. Możliwość oznaczenia terminów jako publiczne i prywatne.
15. Możliwość publicznego udostępniania kalendarzy w trybie do odczytu.

Zadania

1. Możliwość definiowania zadań, ustanowienia daty rozpoczęcia, priorytetu, śledzenia postępu i skuteczności wykonania zadania.
2. Możliwość współdzielenia zadań z użytkownikami wewnętrznymi i zewnętrznymi wraz z ustanowieniem odpowiednich uprawnień (odczyt, zapis).
3. Możliwość dołączania załączników (plików) do poszczególnych zadań.
4. Możliwość synchronizacji zadań, kalendarza, kontaktów na systemach Windows (np. iCAL).
5. Możliwość sortowania zadań (np.: Status, Data).

Pliki

1. Możliwość przechowywania plików, kategoryzacji, podglądania ich zawartości w panelu webowym
2. Możliwość wersjonowania plików.
3. Możliwość tworzenia folderów w których umieszczane są pliki.
4. Możliwość współdzielenia folderów z plikami z użytkownikami wewnętrznymi i zewnętrznymi wraz z ustanowieniem odpowiednich uprawnień (odczyt, zapis).
5. Możliwość zapisu załączników mailowych w folderze plikowym.

Wyszukiwanie

1. Możliwość szybkiego i efektywnego wyszukiwania. Indeksowanie zawartości skrzynki pocztowej po stronie serwera.
2. Interfejs do obsługi konstrukcji zapytań zaawansowanych.
3. Możliwość wyszukiwania dla danego typu elementu (poczty, kontaktów, dokumentów, itp.) lub przez typy elementów.
4. Możliwość wyszukiwania obiektów zawierających: specyficzne słowa kluczowe, utworzonych w określonym okresie czasowym, zawierających załączniki, zawierających załączniki określonego typu, umieszczonych w określonych folderach, w oparciu o rozmiar obiektu, w oparciu o status przeczytany, nieprzeczytany, wysłanych do określonych adresatów, otrzymanych od określonych nadawców, w oparciu o temat, odebranych lub wysłanych z określonej domeny, kontaktów w udostępnionych książkach adresowych, zawartości wewnątrz załączników, terminów w kalendarzach, możliwość wyłączenia przez administratorów indeksowania wiadomości śmieci, wyszukiwania udostępnionych folderów.

**Wymagania funkcjonalne przeglądarkowego klienta pocztowego:**

1. **Funkcje klienta przeglądarkowego**
	1. Aplikacja Web (klient Web) musi być kompatybilna z następującymi przeglądarkami internetowymi:
2. Mozilla Firefox w najnowszej dostępnej wersji na dzień składania ofert.
3. Microsoft w najnowszej dostępnej wersji na dzień składania ofert.
4. Google Chrome w najnowszej dostępnej wersji na dzień składania ofert.
5. Apple Safari w najnowszej dostępnej wersji na dzień składania ofert.
	1. Wszystkie elementy aplikacji muszą posiadać interfejs w języku polskim. Jako element interfejsu, Zamawiający określa również elementy konfiguracji poszczególnych części składowych systemu. W języku polskim są również wyświetlane wszystkie komunikaty przekazywane przez system, włącznie z komunikatami o błędach.
	2. Aplikacja musi dostosowywać rozmiar wszystkich okien do aktualnych ustawień rozdzielczości ekranu.
	3. Zamawiający wymaga, aby dane ze wszystkich formularzy aplikacji do systemu były przesyłane do serwera w postaci zaszyfrowanej (bezpieczny protokół HTTPS/SSL).
	4. Obsługa prostego przeszukiwania musi być oparta na słowach kluczowych z użyciem indeksowania po stronie serwera.
	5. Możliwość przesuwania dynamicznej liczby zaznaczonych obiektów (wiadomości e-mail, dokumenty, pliki, zadania, kontakty, itd.) metodą „przeciągnij i upuść”.
	6. Możliwość automatycznego uzupełniania kontaktów podczas tworzenia lub edycji wiadomości. Adresy powinny być pobierane z zewnętrznej lub wewnętrznej, globalnej bazy adresowej lub bazy adresów użytkownika.
	7. Opcja sprawdzania i poprawiania pisowni w wiadomości e-mail, terminu kalendarza, dokumentów.
	8. Możliwość szybkiego wyświetlania załączników pakietu MS Office oraz pdf w formacie HTML.
	9. Automatyczne grupowanie wiadomości e-mail w wątku, umożliwiające sprawną organizację wiadomości. Wątki e-mail powinny być tworzone niezależnie od lokalizacji wiadomości (np. inny folder).
	10. Możliwość wykonywania operacji (tagowanie, przeciągnij i upuść, usuwanie, itp.) na wątkach wiadomości.
	11. Możliwość przeglądania treści zaznaczonej wiadomości w oknie odczytu.
	12. Możliwość tworzenia folderów osobistych oraz hierarchii folderów. Możliwość zdefiniowania czasu życia wiadomości w poszczególnych folderach w skrzynce pocztowej.
	13. Możliwość sortowania wiadomości na podstawie tematu, daty, nadawcy lub rozmiaru wiadomości e­mail.
	14. Możliwość szybkiej kategoryzacji wiadomości poprzez dodawanie tagów ze zdefiniowanymi przez użytkownika nazwami i kolorami.
	15. Możliwość definiowania przez użytkownika własnych wiadomości o nieobecności. Możliwość definiowania przez użytkownika autoodpowiedzi w zadanym przedziale czasowym.
	16. Możliwość automatycznego zapisu tworzonej wiadomości e-mail. Podczas tworzenia lub odczytywania wiadomości możliwość wyświetlania każdego obiektu w osobnej karcie (zakładce), użytkownik powinien mieć możliwość swobodnego poruszania się pomiędzy kartami (zakładkami).
	17. Możliwość włączenia przez użytkownika automatycznego przekierowania wiadomości przychodzącej na inny adres z możliwością zapisu kopii przekierowywanej wiadomości w podstawowej skrzynce odbiorczej. Możliwość włączenia szybkich powiadomień o otrzymaniu nowej poczty na inny adres e-mail.
	18. Opcja „Odpowiedz”, „Odpowiedz wszystkim” z możliwością zachowania załączników z oryginalnej wiadomości.
	19. Możliwość wybrania wielu wiadomości i wykonania określonej operacji jak na jednej wiadomości np. oznaczenie jako przeczytane.
	20. Wizualizacja przyznanej pojemności konta oraz jej zużycia (za pomocą wskaźnika graficznego).
	21. Możliwość definiowania oraz zmiany przez użytkownika domyślnych preferencji okna odczytu wiadomości e-mail. Użytkownicy mogą ustawić czcionkę domyślną, rozmiar czcionki i kolor czcionki używany do tworzenia wiadomości e-mail oraz dokumentów
	22. Możliwość udostępniania przez użytkowników swoich folderów skrzynki pocztowej i ustanowienia poziomów uprawnień do zarządzania lub tylko do odczytu.
	23. Dostęp do wielu kont wewnętrznych dla uprawnionych użytkowników
	24. Możliwość definiowania przez użytkowników czarnych lub białych list e-mail.
	25. Możliwość dodania komunikatora: wysyłanie szybkich wiadomości typu chat z zastosowaniem bezpiecznego protokołu.
	26. Możliwość zapisywania historii rozmów.
	27. Możliwość konfiguracji dostępności (offline, zaraz wracam, itp.).
	28. Możliwość importu, eksportu konta, kalendarza, kontaktów przez administratora lub użytkownika.
	29. Możliwość przejścia klienta webowego w tryb offline dla przeglądarek Edge lub FireFox lub Chrome (bez podłączenia do serwera poczty).
	30. Możliwość włączenia podwójnego uwierzytelniania użytkowników przy dostępie do usługi web za pomocą dodatkowego kodu pin generowanego z poziomu aplikacji mobilnej w trybie offline.
6. **Funkcje pracy grupowej**
	1. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
	2. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
	3. Mechanizm planowania spotkań z możliwością zapraszania uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
	4. Możliwość udostępniania książek adresowych, zadań z możliwością definiowania poziomów dostępu do zadań, książek.
	5. Mechanizm udostępniania współdzielonych skrzynek pocztowych.
	6. Obsługa list i grup dystrybucyjnych.
	7. Dostęp ze skrzynki do poczty elektronicznej.
	8. Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności.
	9. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
	10. Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.
	11. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych e-mail bez potrzeby wsparcia ze strony pracowników wydziału IT.
	12. Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący prioryteryzacją wyników wyszukiwania.
	13. System powinien umożliwiać użytkownikowi obsługę poczty elektronicznej poprzez przeglądarkę internetową jak również inne programy typu klient poczty e-mail
	14. System powinien umożliwiać przesyłanie wiadomości pocztowych od adresatów zewnętrznych jak i wewnętrznych.
	15. System powinien zapewnić dostęp do skrzynki pocztowej, kalendarza i książek adresowych również za pomocą urządzeń mobilnych obsługiwanych przez dostępne na rynku mobilne systemy operacyjne
	16. System powinien pracować w oparciu o usługi katalogowe LDAP w którym przechowywane są dane konfiguracji usług i skrzynek użytkowników, a także umożliwiać integrację z zewnętrznym katalogiem LDAP,
	17. Usługi katalogowe LDAP systemu muszą być zaimplementowane tak, aby nie było konieczności instalowania dodatkowego oprogramowania na urządzeniach klienckich użytkowników.
	18. System powinien obsługiwać następujące protokoły: SMTP i SMTPS, POP3 i POP3S, IMAP i IMAPS, HTTP (redirect na HTTPS) i HTTPS, CalDAV, CardDAV
	19. System powinien zapewnić w przypadku awarii pojedynczego serwera SMTP, transport elementem redundantnym (MTA, PROXY, itp.) do zewnętrznego serwera SMTP.
	20. Możliwość zdefiniowania w systemie pracy grupowej, wielu domen pocztowych i prowadzenia dla nich kont użytkowników.
7. **Możliwość rozszerzenia funkcjonalności o wsparcie dla użytkowników mobilnych (do ewentualnego wdrożenia w przyszłości)..**
	1. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu.
	2. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem.
	3. System musi zapewniać możliwość korzystania z usług systemu pocztowego (synchronizacja z serwerem) w tym kalendarzy, poczty, zadań, kontaktów przy pomocy urządzeń mobilnych typu PDA, SmartPhone, laptop, tablet pracujących na systemach mobilnych w tym: iOS, Android, Windows Mobile.
	4. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet - z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.
	5. Możliwość synchronizacji automatycznej poczty, zadań, kalendarza i książki adresowej pomiędzy mobilnym klientem pocztowym a serwerem co najmniej dla 25 użytkowników.
8. **Funkcjonalność klienta offline**

4.1 Możliwość współpracy z programem Microsoft Outlook w wersjach 2013, 2016, 2019, zapewniająca dwustronną synchronizację poczty, kontaktów i kalendarza między programem Microsoft Outlook, a serwerem.

4.2 Możliwość przechowywania wiadomości w programie Microsoft Outlook w trybie offline.

Możliwość automatycznej konfiguracji i dostępu do globalnej książki adresowej pomiędzy programem Microsoft Outlook a serwerem.

* 1. Możliwość bezpiecznego połączenia przez HTTPS, szyfrowanie całego ruchu między

programem Microsoft Outlook a serwerem.

* 1. Możliwość udostępnienia kalendarza wraz z odpowiednimi uprawnieniami, za pomocą

programu Microsoft Outlook wraz z podglądem wolny/zajęty dla innych użytkowników systemu oraz podłączenia w swoim widoku kalendarzy udostępnionych przez innych.

* 1. Możliwość udostępnienia folderu pocztowego innym użytkownikom systemu oraz podłączenia

w swoim widoku udostępnionych przez innych użytkowników folderów pocztowych.

* 1. Możliwość synchronizacji zadań utworzonych w programie Microsoft Outlook.
	2. Możliwość synchronizacji kontaktów utworzonych w programie Microsoft Outlook
	3. Możliwość dodawania stopek adresowych i ich synchronizacja z serwerem.
	4. Możliwość pobierania z serwera tylko nagłówka wiadomości.
	5. Automatyczne wykrywanie stanu połączenia online/offline bez konieczności ingerencji

użytkownika w zmianę statusu.

* 1. Możliwość automatycznej, dwukierunkowej synchronizacji kategorii (tagów) wiadomości

między programem Microsoft Outlook, a serwerem.

* 1. Możliwość automatycznego opóźniania wysłania wiadomości ze skrzynki użytkownika
	2. Możliwość ustawienia i synchronizacji z serwerem informacji o nieobecności.
	3. Możliwość sprawdzenia pojemności skrzynki oraz jej zajętości na serwerze z poziomu

programu Outlook.

* 1. Możliwość dodania pełnomocników, czyli osób, które mogą wysyłać pocztę „w imieniu” lub

„jako” użytkownik. Synchronizacja tej informacji z serwerem.

* 1. Możliwość dodanie, edycji i synchronizacji z serwerem reguł poczty pozwalające na różne

operacje na przychodzących mailach (np. przenieś do folderu, oznacz wiadomość, prześlij ją dalej), na podstawie ustawionych filtrów (np. temat, pole DO, DW).

1. **Zarządzanie i bezpieczeństwo systemu**
	1. Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk.
	2. Definiowanie rozmiaru skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.
	3. Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników.
	4. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer.
	5. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań - na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych - bez przyznawania pełnych uprawnień administracyjnych.
	6. Mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów audytowych.
	7. Wiadomości oznaczone przez użytkowników jako SPAM lub NIE SPAM są automatycznie dodawane do silnika szkolenia antyspamowego.
	8. Możliwość blokowania załączników na podstawie takich kryteriów jak: rodzaj i rozmiar załączników.
	9. Wsparcie dla technologii hierarchicznego przechowywania danych, czyli umożliwiającej przeniesienie danych użytkownika z zasobów szybkich na wolniejszy storage po spełnieniu warunku czasowego.
	10. Możliwość zainstalowania i zarządzania certyfikatami z konsoli administracyjnej.
	11. Możliwość tworzenia/planowania backupu środowiska oprogramowania.
	12. Możliwość realizowania kopii /odzyskiwania pojedynczej skrzynki lub zestawu skrzynek w sposób pozwalający na zachowanie dostępności i ciągłości pracy.
	13. Zapewnienie pełnej redundancji serwerów poczty elektronicznej w ramach dostarczanego przez Zamawiającego programowania do wirtualizacji, w taki sposób aby żaden pojedynczy punkt awarii nie powodował zatrzymania pracy systemu oraz jego kluczowych funkcjonalności.
	14. Możliwość tworzenia dodatkowych (redundantnych) serwerów w celu podniesienia wydajności środowiska i zapewniania ciągłości działania (architektura HA - High Availability).
	15. Umożliwienie przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie - nawet w godzinach pracy biurowej bez zakłócenia pracy użytkowników.
2. **Funkcje organizacji danych**
	1. Możliwość definiowania zasad przechowywania: wszystkich wiadomości, wiadomości śmieci, wiadomości do odzyskania oraz wiadomości usuniętych.
	2. Możliwość przeniesienia skrzynki pocztowej lub pocztowych z jednego serwera na drugi bez konieczności przestojów systemu lub generowania zdarzeń mających wpływ na działanie innych skrzynek.
	3. Możliwość włączenia funkcji odzyskiwania przez użytkownika usuniętych elementów, w określonym przez administratora systemu czasie.
3. **Funkcje administracji systemem**
	1. Możliwość administracji systemem przez interfejs przeglądarkowy i klasyczną linię komend (Command Line Interface).
	2. Możliwość tworzenia i zarządzania wieloma domenami w ramach jednej instancji serwera.
	3. Możliwość korzystania z różnych globalnych list adresowych dla każdej z domen.
	4. Możliwość przyznania określonej przestrzeni dyskowej dla określonej domeny.
	5. Możliwość przyznania określonej przestrzeni dyskowej dla określonego konta.
	6. Możliwość przeniesienia domeny.
	7. Możliwość przeszukiwania skrzynek pocztowych z poziomu konsoli administracyjnej na podstawie kwerendy wyszukiwania, z możliwością wybrania wszystkich lub tylko grupy kont pocztowych do przeszukania. Wyniki zapisywane są jako kopie wiadomości, na zdefiniowanej w zapytaniu skrzynce pocztowej, w wybranym folderze docelowym. System musi umożliwiać nadawanie uprawnień do przeszukiwania treści skrzynek dla wybranych użytkowników.
	8. Możliwość przypisania użytkownikowi zastępczego adresu e-mail (aliasu).
	9. Możliwość tworzenia grup dystrybucyjnych wiadomości e-mail.
4. **Funkcje edycji dokumentów**
	1. System powinien mieć możliwość edycji dokumentów Office: dokument tekstowy, arkusz kalkulacyjny, prezentacja.
	2. Moduł edycji dokumentów jest dostępny w panelu webowym i pozwala na edycję dokumentów już zapisanych i tworzenie nowych, zapisywanych w folderach plikowych.
	3. Moduł powinien mieć wsparcie minimum dla podstawowych formatów MSOffice: .doc, .xls i .ppt
5. **Funkcje archiwum pocztowego (poza natywną funkcjonalnością systemu)**
	1. Archiwum pocztowe musi umożliwiać realizację polityk składowania i dostępu do danych archiwalnych w dwóch wariantach:
6. W archiwum są umieszczone wszystkie dane poczty przychodzącej/wychodzącej wraz z załącznikami.
7. Każdy użytkownik systemu za pomocą panelu web interfejsu systemu poczty elektronicznej może samodzielnie wykonać operację przeniesienia jednej bądź wielu wiadomości do systemu archiwum z możliwością pozostawienia wiadomości na swoim profilu bądź jej skasowania po przesłaniu do archiwum.
	1. Użytkownik systemu może w panelu web interfejsu poczty wskazać samodzielnie, czy poczta ma być archiwizowana automatycznie i jak ma działać mechanizm kwalifikacji (data) wiadomości do automatycznej archiwizacji.
	2. System archiwizacji poczty musi posiadać dedykowany panel web dla użytkowników systemu, w którym mogą oni wykonać operacje: filtrowania wiadomości, oznaczania ich tagami, przesłania wiadomości do swojego konta pocztowego.
	3. System archiwizacji poczty musi posiadać dedykowany interfejs administratora umożliwiający:
8. tworzenie użytkowników
9. tworzenie grup
10. dodawanie domen
11. tworzenie zasad archiwizacji
12. tworzenie zasad retencji
13. tworzenie schematów wyszukiwania automatycznego
14. przeglądanie statystyk archiwum
15. informacje na temat stanu systemu audyt (informacje na temat operacji jakie użytkownicy wykonywali w systemie)
	1. Możliwości konfiguracyjne systemu archiwizacji:
16. Integracja z AD.
17. Logowanie użytkowników na podstawie danych z domeny LDAP Zimbra, Exchange, Lotus, etc.
18. Integracja przy wykorzystaniu IMAP.
19. Logowanie poprzez autentykację IMAP na głównym serwerze pocztowym.
20. Przywracanie poczty przy wykorzystaniu protokołu IMAP.
21. Integracja przy wykorzystaniu POP3.
22. Logowanie poprzez autentykację POP3 na głównym serwerze pocztowym.
23. Integracja z google authenticator.
24. Pełna integracja archiwum pocztowego z oferowanym systemem poczty i pracy grupowej.
25. 3 tryby archiwizacji poczty: manualny, użytkownika i zaplanowany.
26. Elastyczna konfiguracja na poziomie: użytkownika, klasy usług oraz administratora.
27. Zintegrowane zarządzanie archiwum z panelem administracyjnym systemu poczty i pracy grupowej.
28. Dedykowana zakładka archiwum w panelu WWW użytkownika.
29. Obsługa SSO (pomiędzy serwerem archiwum a Zimbrą).
30. Raporty o stanie zrealizowanych zadań archiwizacji dla administratora.
31. Podgląd zrealizowanych zadań archiwizacji dla użytkownika (online).
32. Wsparcie dla instalacji wieloserwerowych.
33. Możliwość włączenia/wyłączenia kosza użytkownika z obsługi archiwum.
34. Możliwość ustawienia daty ograniczającej dostęp użytkownika do danych archiwalnych poczty.

Funkcjonalność ma być dostępna minimum przez okres minimum 36 miesięcy.

1. **Funkcje mechanizmu resetu hasła w AD z poziomu panelu www użytkownika (poza natywną funkcjonalnością systemu)**

Możliwość wykonania resetu hasła użytkownika w Active Directory (AD) z poziomu panelu poczty użytkownika.

**Kilkuetapowa zmiana hasła:**

* Ekran z podaniem emaila i numeru telefonu.
* Generowanie tokenu autoryzacyjnego i przesłanie do użytkownika poprzez mechanizm SMS.
* Ekran walidacji podanego tokenu.
* Ekran informacji o sukcesie podczas zmiany hasła poprzez sms.
* System posiada zabezpieczenia przed podaniem niepoprawnych danych.
* System posiada walidację numeru telefonu oraz emaila.
* System umożliwia zmianę hasła zarówno w AD jak i hasła lokalnego.
* System automatycznie wykrywa ustawiony mechanizm autoryzacji użytkownika.
* Moduł jest w pełni zintegrowany z systemem pocztowym (system extension) oraz umożliwia przejście do mechanizmu zmiany hasła bezpośrednio z panelu logowania użytkownika.

**Funkcjonalność od strony Panelu administratora:**

* Włączenie/Wyłączenie przycisku “Zapomniałem hasła – sms”.
* Konfiguracja bramki SMS (zewnętrzny serwis np: SMSAPI).
* Definiowanie czasu życia tokenu.
* Definiowanie tekstu sms’a z tokenem (umożliwiając podanie zmiennych z wartościami użytkownika, tokenu itd.).
* Definiowanie tekstu sms’a z nowym hasłem (obsługa zmiennych).
* Możliwość wyboru domeny, którą obowiązuje możliwość zmiany hasła przez sms.
* Konfiguracja aktywacji/deaktywacji modułu na podstawie domeny.
* Obsługa możliwego do włączenia fallbacka – zmiana hasła zarówno lokalnie jak i w AD, w przypadku gdy zmiana hasła w AD się nie powiedzie (np. przez brak konta).
* Wyświetlanie konfiguracji podłączonego AD lub informację o autoryzacji lokalnej.
* Pełna obsługa powiadomień o każdym z etapów resetu hasła (w interfejsie administratora) – kto i kiedy rozpoczął resetowanie hasła, kiedy je zakończył, czy się powiodło.
* Możliwość definiowania interwału kasowania powiadomień.

Funkcjonalność ma być dostępna przez okres minimum 36 miesięcy.

**11. Realizacja wdrożenia z migracją danych**

Wykonawca opracuje koncepcję architektury dla systemu pocztowego uwzględniając obecne środowisko Klienta i dodatkowe wymagania dotyczące bezpieczeństwa wdrażanego systemu.

Instalacja i konfiguracja serwera dostarczanego przez oferenta, systemu operacyjnego oraz systemu poczty i pracy grupowej z uwzględnieniem:

1. Integracji dostarczanego systemu z ActiveDirectory.
2. Utworzenie kont, aliasów, kont grupowych.
3. Konfigurację zabezpieczeń: AV/AS, Whitelisting i blacklisting, DKIM, SPF, DMARC, CBPOLICYD.
4. Konfigurację systemu do współpracy z urządzeniami brzegowymi LAN.

Zaimplementowanie polityki backup obejmującej:

1. Tworzenie kopii środowiska i danych wykorzystanych do szybkiego uruchomienia systemu zapasowego w przypadku sytuacji krytycznych (Disaster Recovery).
2. Tworzenie kopii zapasowych pełnych danych użytkowników.
3. Tworzenie kopii zapasowych przyrostowych danych użytkowników.

 Migracja danych pocztowych:

* + 1. Zrealizowanie migracji danych pocztowych z obecnego serwera poczty elektronicznej na nowy serwer poczty.

Utworzenie przez Wykonawcę dokumentacji powdrożeniowej dla serwera poczty uwzględniającą opis architektury i zabezpieczeń.

**12. Realizacja szkolenia administracyjnego**

Kurs w formie warsztatowej obejmujący zagadnienia związane z tematem instalacji, zarządzania
i prac konserwacyjnych dla oferowanego systemu.

Kurs szkoleniowy musi obejmować minimum:

1. Przeszkolenie z architektury systemu.
2. Wdrożenie w proces instalacji systemu.
3. Rozwiązywanie problemów podczas instalacji.
4. Obsługa konsoli administracyjnej.
5. Korzystanie z narzędzi CLI.
6. Korzystanie z narzędzi służących do monitoringu systemu, logów systemowych.
7. Realizacja polityki backupu.
8. Korzystanie z podpowiedzi w systemie.
9. Zagadnienia związane z migracją kont pocztowych.

j) Zabezpieczenia systemu AV/AS.

k) Integracja usług Active Directory.

l) Konfiguracji i administrowania systemem archiwum pocztowego.

* Czas trwania szkolenia: 4 spotkania po 4 godziny.
* Liczba administratorów do przeszkolenia: 3 osoby.
* Materiały szkoleniowe: każdy z uczestników otrzyma materiały szkoleniowe w formie elektronicznej oraz certyfikat ukończenia kursu.
* Miejsce szkolenia: zdalnie.

# Wdrożenia zaawansowanego systemu antyspamowego

# Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

# Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

# Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

# Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

# Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

# Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

# Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

# Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

# Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

# Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

# Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

# Serwisy i licencje

System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

# Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

# Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca 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.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.