Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

„System Bezpiecznej Poczty Firmowej"

1. Przedmiot Zamówienia

Przedmiotem zamówienia jest dostawa niezbędnych licencji oraz wykonanie wdrożenia i konfiguracji Systemu Bezpiecznej Poczty Firmowej w środowisku produkcyjnym Zamawiającego, zgodnie z Harmonogramem Wdrożenia, a także realizacja uprawnień Zamawiającego wynikająca z Gwarancji Producenta i Gwarancji Wykonawcy oraz świadczenie usług Asysty Powdrożeniowej.

2. Ramowy harmonogram dostawy i konfiguracji Systemu Bezpiecznej Poczty Firmowej.

ETAP I - Rozpoczęcie projektu, analiza zakresu i przygotowanie planu projektu uwzględniającego ciągłość działania Zamawiającego.

1. Przeprowadzenie analizy przedwdrożeniowej istniejącego sposobu korzystania z poczty elektronicznej przez Zamawiającego.
2. Przygotowanie projektu Systemu BPF poczty w ramach infrastruktury IT Zamawiającego.
3. Opracowanie szczegółowego harmonogramu wdrożenia i konfiguracji Systemu BPF oraz przedstawienie go do akceptacji Zamawiającego. Harmonogram musi uwzględniać wymagania ramowe Zamawiającego.

ETAP II – Konfiguracja rozwiązania w ramach infrastruktury IT Zamawiającego w Rzeszowie oraz migracja skrzynek pocztowych w sposób zapewniający ciągłość działania Zamawiającego.

1. Wykonanie konfiguracji środowiska serwerowego i licencji w ramach infrastruktury IT.
2. Przygotowanie planu i metod migracji.
3. Wykonanie migracji testowych oraz poddennie ich weryfikacji.
4. Wykonanie migracji produkcyjnej – docelowej i jej weryfikacja.
5. Wdrożenie i uruchomienie dodatkowych modułów, w tym zabezpieczeń poczty.

ETAP III - Odbiór Końcowy potwierdzający uzyskanie pełnej funkcjonalności i zabezpieczeń dla Systemu Bezpiecznej Poczty Firmowej.

1. Dostarczenie niezbędnych licencji wymaganych do uzyskania pełnej funkcjonalności Systemu BPF.
2. Dostarczenie dokumentacji powdrożeniowej.

ETAP IV - Asysta powdrożeniowa w liczbie godzin oraz na warunkach wskazanych w OPZ i Umowie.

Łączny czas wdrożenia tj. realizacji Etapów I-III nie może przekroczyć być krótszy niż 30 i dłuższy niż 45 Dni Kalendarzowych od rozpoczęcia realizacji Etapu I.

3. Dostawa, wdrożenie i uruchomienie Systemu Bezpiecznej Poczty Firmowej

3.1. Stan obecny

1) Zamawiający posiada obecnie 500 skrzynek (w różnych domenach, skrzynki archiwalne) łącznie wykorzystywanych przez ok. 250 użytkowników oraz 50 dostępów technicznych wykorzystywanych przez systemy.
2) Zamawiający posiada skrzynki współdzielone, kluczowe, operacyjne oraz skrzynki pracowników.
3) Zamawiający posiada obecnie pocztę na hostingu home.pl.
4) Zamawiający posiada stworzoną hybrydę część poczty została przekierowana na skrzynki MS Exchange on-line w ilości ok. 100 szt.
5) Na hostingu zamawiającego obecnie jest utworzonych ok. 20 grup mailingowych.
6) Obecnie wykorzystana przestrzeń na skrzynki mailowe wynosi ok 1.3 TB
7) Zamawiający posiada kilka skrzynek o powierzchni powyżej 25 GB max do 100GB.

3.2. Stan docelowy

1) Zamawiający w ramach postępowania wymaga dostarczenia wymaganych licencji, wdrożenia kompletnego Systemu BPF, migracji zasobów poczty elektronicznej Zamawiającego (home.pl) oraz z usługi Microsoft Exchange on-line do Systemu BPF w sposób zapewniający ciągłość działania Zamawiającego.
2) System BPF musi funkcjonować na w ramach wirtualizacji stosowanej u Zamawiającego.
3) W powyższym celu Zamawiający udostępni niezbędne maszyny wirtualne z adekwatną konfiguracją (rekomendowana liczba vCPU, RAM, systemem operacyjny spośród systemów Debian / Ubuntu lub Windows Server), a także niezbędną przestrzeń dyskową (dyski NVME/SSD oraz HDD w ramach posiadanych macierzy dyskowych). Parametry serwerów wirtualnych oraz sposób organizacji przestrzeni dyskowych zostaną ustalone w ramach Etapu I.
4) Wybór systemu operacyjnego należy do Wykonawcy, spośród podanych w § 4.2 pkt.3, jego instalacja i konfiguracja wraz z niezbędnymi komponentami, w tym z modułem bezpieczeństwa poczty, jest przedmiotem działań Wykonawcy w uzgodnieniu z Zamawiającym.
5) Konfiguracja i wdrożenie modułu bezpieczeństwa poczty.
6) Integracja z rozwiązaniem LDAP Zamawiającego tj. kontrola uprawnień z poziomu Microsoft Active Directory umieszczonego w infrastrukturze IT Zamawiającego.
7) Integracja z posiadanymi przez Zamawiającego systemami tj. usługami DNS, bramą antyspamową i antywirusową, systemem logowania SYSLOG (Gray LOG), Zabbix, Forti Analyser.
8) Dostosowanie szaty graficznej panelu webowego do kolorystyki i marki Zamawiającego.
9) Dostarczenie niezbędnej dokumentacji powykonawczej w formatach docx oraz pdf.

3.3. Przeprowadzenie migracji do Systemu BPF – kluczowe wytyczne.

1) Migracja danych będzie realizowana z systemu poczty Zamawiającego (home.pl oraz Microsoft Exchange on-line) – dalej system źródłowy.
2) Wykonawca jest odpowiedzialny za współpracę z Home.PL w celu efektywnej organizacji procesu migracji.
3) Za przeniesienie danych z systemu źródłowego do Systemu BPF odpowiada Wykonawca.
4) Wszystkie prace związane z poprawnym przeprowadzeniem migracji danych wykonywane będą w taki sposób, aby zapewnić płynność pracy Zamawiającego zgodnie z planem migracji opracowanym w ramach szczegółowego harmonogramu wdrożenia Systemu BPF.

5) Metody weryfikacji poprawności danych w procesie migracji oraz kryteria ich odbioru, muszą być szczegółowo ustalone w ramach projektu rozwiązania oraz zweryfikowane i w razie potrzeby zaktualizowane bezpośrednio przed rozpoczęciem migracji poszczególnych zbiorów. Wykonawca musi również zaprojektować i zaimplementować narzędzia (skrypty i raporty) umożliwiające zastosowanie wyspecyfikowanych metod weryfikacji danych.
6) W przypadku stwierdzenia błędów w danych źródłowych, które skutkowałyby na poprawność procesu migracji, Wykonawca jest zobowiązany do przeprowadzenia wspólnie z Zamawiającym procesu poprawy danych w systemach źródłowych, o ile wcześniejsza analiza danych w systemach źródłowych wykaże taką potrzebę. W ramach procesu poprawy danych w systemach źródłowych, Wykonawca będzie wspierał Zamawiającego poprzez tworzenie skryptów i innych narzędzi pozwalających na poprawę danych. Jeżeli na skutek analizy okaże się, że jedyną formą poprawy danych jest ich ręczna edycja wówczas, takiej poprawy dokona Zamawiający w swoich systemach źródłowych.
7) Wykonawca jest zobowiązany do opracowania narzędzi i mechanizmów służących migracji danych i ich stałej aktualizacji o ile zachodzi taka potrzeba, tj. na skutek prowadzonych analiz przedwdrożeniowych, migracji próbnych czy testów.
8) Wykonawca po dokonaniu weryfikacji struktur danych w systemie źródłowym, poprawy danych w systemie źródłowym dokona migracji danych (co najmniej testowej i produkcyjnej) do Systemu BPF.
9) Plan migracji musi zostać uzgodniony pomiędzy stronami co najmniej na 5 Dni Roboczych przed planowaną datą rozpoczęcia, za opracowanie którego odpowiada Wykonawca.
10) Przeprowadzenie migracji skrzynek pocztowych co najmniej w zakresie:
    - wiadomości pocztowych (otrzymanych i wysłanych) z zachowaniem zastanej struktury folderów na każdym z kont;
    - kontaktów;
    - archiwalnych i przyszłych zdefiniowanych wydarzeń zarejestrowanych w kalendarzach użytkowników.
11) Wykonanie testów migracji dla wskazanych przez Zamawiającego użytkowników.
12) Włączenie funkcji samoobsługowej zmiany hasła:
    - Udostępnienie portalu do samoobsługowej zmiany hasła, np. Microsoft Self-Service Password Reset (SSPR) lub inny równoważny.
    - Po zmianie hasła w portalu, użytkownicy automatycznie odzyskują dostęp do oferowanego systemy poczty.
13) Integracja z Active Directory tj. możliwość zakładania i blokowania kont z poziomu AD z uwzględnieniem rozgraniczenia skrzynek zakładanych z poziomu AD oraz z poziomu panelu administratora.
14) Skonfigurowanie funkcjonalności centralnego zarządzania stopkami (podpisami tj. Dane osobowe, stanowisko, dane kontaktowe, logo oraz informacja prawna) w oparciu oparciu o LDAP / AD.
15) Dla każdego migrowanego konta należy dostarczyć raport w postaci logu zawierającego ilość przekopiowanych wiadomości, wpisów książki adresowej, ewentualne błędy, itp.

3.4. Konfiguracja i wdrożenie modułu bezpieczeństwa poczty.

Moduł bezpieczeństwa poczty e-mail powinien zapewniać kompleksową ochronę serwera pocztowego.

1) Ochrona serwera pocztowego:

- Zaawansowana ochrona antyspamowa oparta na filtrach reputacyjnych, analizie heurystycznej i mechanizmach uczenia maszynowego, z możliwością dostosowania do specyficznych potrzeb organizacji.
- Funkcje antywirusowe umożliwiające skanowanie wiadomości e-mail i załączników w celu wykrywania i blokowania złośliwego oprogramowania, w tym ransomware, wirusów oraz phishingu.
- Mechanizmy zapobiegania wyciekom danych (DLP) poprzez monitorowanie treści wiadomości i załączników, z możliwością identyfikacji wrażliwych danych i wdrażania polityk bezpieczeństwa.

2) Integracja z systemami analizy i monitorowania:
   - Możliwość integracji z narzędziami do centralnego zarządzania i analizy danych, takimi jak systemy logowania i monitorowania oraz platformy SIEM, np. Forti Analyzer, Graylog oraz Zabbix.
   - Automatyczne przesyłanie danych o zdarzeniach i raportów do centralnych systemów analitycznych.
   - Integracja z rozwiązaniem Fortigate UTM, które posiada Zamawiający tj. wdrożonym u Zamawiającego w jego Infrastrukturze IT.
3) Oznaczanie wiadomości pod kątem bezpieczeństwa:
   - Automatyczne oznaczanie wiadomości zawierających potencjalne zagrożenia poprzez dodawanie tagów, zmiany w temacie wiadomości lub dostarczanie ostrzeżeń w treści e-maili.
   - Możliwość dostosowania reguł oznaczania do polityk organizacyjnych.
4) Zarządzanie regułami i politykami pocztowymi:
   - Możliwość konfiguracji reguł przekierowania wiadomości na podstawie ich treści, nadawcy, odbiorcy lub załączników.
   - Obsługa kwarantanny wiadomości, przekierowania do administratorów bezpieczeństwa oraz polityk blokowania/akceptowania.
   - Funkcjonalność zarządzania przepływem wiadomości i priorytetyzacji na podstawie zdefiniowanych kryteriów.
5) Wysoka wydajność i niezawodność:
   - Skalowalność rozwiązania umożliwiająca obsługę rosnącej liczby wiadomości i użytkowników.
   - Wsparcie dla wdrożenia w środowiskach lokalnych (on-premises) w formie maszyny wirtualnej.
6) Zaawansowane funkcje ochrony przed zagrożeniami:
   - Wykrywanie zaawansowanych ataków typu BEC (Business Email Compromise) oraz spear phishing.
   - Analiza behawioralna i sandboxing dla załączników i linków zawartych w wiadomościach.
   - Funkcje automatycznego przywracania wiadomości po incydentach ransomware.
   - Mechanizm Content Disarm and Reconstruction (CDR): Usuwanie aktywnych treści z załączników, np. makr w dokumentach, aby zminimalizować ryzyko ataków.
7) Dostosowanie do wymagań prawnych i polityk bezpieczeństwa:
   - Możliwość wprowadzenia polityk zgodnych z wymaganiami prawnymi dotyczącymi ochrony danych, takich jak RODO.
   - Wsparcie dla szyfrowania wiadomości oraz zabezpieczeń protokołów SMTP.

4. Wymagania dla oprogramowania Modułu Serwera Poczty

Oprogramowanie Serwer Poczty musi charakteryzować się następującymi wbudowanymi cechami tj. pochodzącymi od jednego producenta i stanowiącymi spójne rozwiązanie. Przedstawione wymagania są wymaganiami minimalnymi.

4.1. Liczba licencji / kont

Dostarczenie bezterminowych licencji Modułu Serwera Poczty Firmowej, uprawniającej Zamawiającego do utrzymywania **300 jednoczesnych** Skrzynek Pocztowych użytkowników (mogą być współużytkowane przez wielu użytkowników) oraz ze wsparciem technicznym producenta Modułu Serwera Poczty, uprawniającym Zamawiającego do uzyskiwania aktualizacji Modułu Serwera Poczty przez okres 36 miesięcy od zakończenia wdrożenia potwierdzonego Protokołem Odbioru Końcowego.

4.2. Wymagania funkcjonalne podstawowe

1) Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych z mechanizmem powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
2) Automatyczne grupowanie wiadomości e-mail w wątku, umożliwiające sprawną organizację wiadomości. Wątki e-mail powinny być tworzone niezależnie od lokalizacji wiadomości (np. inny gdy zostały przeniesione do innego folderu). Możliwość operacji na całych wątkach (oznaczanie, usuwanie, przeciąganie do innego folderu).
3) Tworzenie i zarządzanie osobistymi i udostępnionymi kalendarzami oraz listami kontaktów, możliwość tworzenia wielu list kontaktów oraz grup kontaktów przez użytkownika w ramach jednego konta.
4) Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z opcjonalnym przypisaniem terminu i przypomnienia (wtedy mail staje się zadaniem) – tj. możliwość tworzenia zadania z wiadomości pocztowej z poziomu klienta WWW.
5) Możliwość zablokowania przesłania i przekazywania wiadomości do domen zewnętrznych.
6) Możliwość jednoczesnej, bezawaryjnej pracy 300 użytkowników. Przy czym użytkownicy łączą się do serwera za pomocą klienta WWW lub innego oprogramowania opartego o standardowe protokoły: IMAP i IMAPS, SMTP i SMTPS, POP3 i POP3S, CalDAV i CardDAV.
7) System pocztowy musi być skalowalny do obsługi 600 kont użytkowników lub więcej, przy wykorzystaniu dodatkowego sprzętu np. poprzez zwiększenie parametrów maszyn wirtualnych (vCPU, RAM).
8) Pełne wsparcie Systemu BPF dla klienta poczty elektronicznej MS Outlook w wersjach 2016 i nowszych.
9) System musi być zabezpieczony przed lukami bezpieczeństwa wynikającymi z technologii, w której został stworzony.
10) Możliwość wysyłania zaszyfrowanych wiadomości e-mail.
11) Możliwość wykorzystania Microsoft Active Directory do uwierzytelniania użytkowników, prezentacji listy użytkowników w globalnej książce adresowej i SSO.
12) System powinien pracować w oparciu o usługi katalogowe LDAP (bez konieczności instalowania dodatkowego oprogramowania na urządzeniach klienckich), w których przechowywane są dane konfiguracji usług i skrzynek użytkowników, a także umożliwiać

integrację z zewnętrznym katalogiem LDAP do uwierzytelniania użytkowników i prezentacji listy użytkowników w globalnej książce adresowej.
13) System musi posiadać możliwość integracji z rozwiązaniami Zoom, MS OneDrive, MS Teams oraz rozwiązaniem NextCloud posiadanym przez Zamawiającego.
14) Panel WWW musi spełniać zasady tworzenia responsywnych aplikacji webowych, zapewniając użytkownikom spójne wrażenia i pełną funkcjonalność na wszystkich urządzeniach desktop, tablet oraz smartfon tj. dostosowywać się do urządzeń na których jest wyświetlany, zachowując ergonomię i funkcjonalność.
15) Panel WWW musi być skonstruowany jako progresywna aplikacja internetowa (PWA) uruchamiana tak jak zwykła strona internetowa, ale umożliwiająca stworzenie wrażenia działania jak natywna aplikacja mobilna lub aplikacja desktopowa. PWA może zostać zainstalowana, wtedy może posiadać własną ikonę na pulpicie oraz być niezależna od przeglądarki.
16) Możliwość drukowania wiadomości oraz wyświetlania podglądu wydruku. Możliwość wyboru i drukowania wielu wiadomości jednocześnie.
17) Możliwość definiowania reguł filtrowania i priorytetów dla wiadomości przychodzących i wychodzących.
18) Możliwość stosowania nowych reguł na istniejących wiadomościach.
19) Możliwość definiowania własnego podpisu oraz konfiguracji przez administratorów maksymalnej liczby znaków używanych w podpisach.
20) Prezentowanie wiadomości poczty elektronicznej użytkownika z poziomu interfejsu webowego w widoku wg kolejności napływania lub grupującym w konwersacje.
21) Możliwość zdefiniowania priorytetu wysyłanej wiadomości pocztowej.
22) Możliwość załączania definiowalnej przez administratora liczby załączników do wysyłanej wiadomości elektronicznej o rozmiarze maksymalnym definiowalnym przez administratora
23) Pobieranie dużej ilości załączników wiadomości elektronicznej w postaci jednej paczki (np. skompresowanego archiwum zip).
24) Wyświetlanie użytkownikowi bieżącej zajętości przestrzeni skrzynki użytkownika.
25) Możliwość oznaczenia wiadomości flagą lub znacznikami definiowanymi przez użytkownika umożliwiającymi grupowanie szybsze wyszukiwanie wiadomości.
26) Obsługa funkcjonalności drag&drop w interfejsie webowym w zakresie przenoszenia wiadomości, dokumentów, plików, w tym po więcej niż jednego na raz.
27) Interfejs webowy do obsługi poczty powinien umożliwić użytkownikowi tworzenie wiadomości przez edytor WYSWIG z możliwością stosowania rożnego rodzaju formatowań, krojów czcionek, styli itp.
28) Sprawdzanie i poprawiania pisowni w wiadomości e-mail, terminu kalendarza, dokumentów.
29) Umożliwienie użytkownikowi wysyłanie wiadomości w formacie tekstowym lub HTML.
30) Automatyczne podpowiadanie adresu odbiorcy z dostępnych książek adresowych podczas tworzenia wiadomości, w tym z zewnętrznej lub wewnętrznej, globalnej bazy adresowej lub bazy adresów użytkownika.
31) 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.
32) 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.

33) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi ustawienie żądania potwierdzenia odbioru wiadomości przez odbiorcę.
34) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi zmianę hasła na żądanie oraz wg polityki złożoności zdefiniowanej przez administratora
35) Możliwość zablokowania konta użytkownika po określonej liczbie nieudanych prób logowania w zadanym okresie czasu.
36) Możliwość zdefiniowania podpisu użytkownika dołączanego automatycznie do każdej nowej wysyłanej wiadomości.
37) Możliwość odzyskania skasowanej przez użytkownika wiadomości z folderu „kosz" z poziomu interfejsu webowego.
38) Możliwość szybkiego i efektywnego wyszukiwania w systemie tj. wdrożenie indeksowania zawartości skrzynki pocztowej po stronie serwera.
39) Obsługa innych aplikacji za pomocą interfejsów SOAP/REST/API poprzez udostępnianie usług (np. Web-services) oraz dostęp do API programistycznego za pomocą którego można integrować się z systemami trzecimi.
40) Dostęp do wielu kont wewnętrznych dla uprawnionych użytkowników.

4.3. Dodatkowe funkcjonalności dot. klienta webowego (panel WWW) i mobilność

1) Aplikacja Web (klient webowy) musi być kompatybilna z następującymi przeglądarkami internetowymi: Mozilla Firefox, Microsoft Edge, Google Chrome oraz Apple Safari, w najnowszych dostępnych wersjach na dzień składania oferty.
2) 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.
3) Dane klienta webowego mają być przesyłane do serwera poczty w postaci zaszyfrowanej z wykorzystaniem bezpiecznego protokół HTTPS/SSL.
4) Możliwość przeglądania treści zaznaczonej wiadomości w oknie odczytu.
5) Możliwość szybkiego wyświetlania załączników pakietu MS Office oraz plików pdf w formacie HTML oraz możliwość zapisu załączników mailowych w folderze plikowym.
6) Możliwość tworzenia folderów osobistych oraz hierarchii folderów.
7) Możliwość tworzenia i współdzielenia folderów (z ustanawianiem uprawnień do odczytu zapisu), w których umieszczane są pliki; wersjonowanie i kategoryzowanie plików;
8) Możliwość zdefiniowania czasu życia wiadomości w poszczególnych folderach w skrzynce pocztowej.
9) Możliwość sortowania wiadomości na podstawie tematu, daty, nadawcy lub rozmiaru wiadomości e-mail oraz możliwość prostego i zaawansowanego (tj. wielokryterialnego) wyszukiwania danego typu obiektu np. wiadomości, kontaktów, plików dokumentów itp.
10) Możliwość wyszukiwania obiektów dostępnych w Systemie BPF:
    - na podstawie wskazanych słów kluczowych oraz ze względu na rozmiar i temat;
    - utworzonych (w tym wysłanych, odebranych) w określonym przedziale czasu;
    - zawierających załączniki – w tym załączniki określonego typu;
    - umieszczonych w określonych folderach lub oznaczonych określonymi tagami;
    - w oparciu o status przeczytany, nieprzeczytany, wysłanych do określonych adresatów, otrzymanych od określonych nadawców, odebranych lub wysłanych z określonej domeny;
    - kontaktów w udostępnionych książkach adresowych, udostępnionych folderów;

- zawartości wewnątrz załączników, wyszukiwanie terminów w kalendarzach;
- możliwość wyłączenia przez administratorów indeksowania wiadomości „śmieci".

11) Funkcjonalność automatycznego dostosowywania się wyników wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący odpowiednim sortowaniem wyników wyszukiwania na podstawie częstotliwości wyszukiwania / korzystania.
12) Możliwość szybkiej kategoryzacji wiadomości poprzez dodawanie tagów ze zdefiniowanymi przez użytkownika nazwami i kolorami.
13) 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).
14) Opcja „Odpowiedz", „Odpowiedz wszystkim" z możliwością zachowania załączników z oryginalnej wiadomości.
15) Możliwość wybrania wielu wiadomości (wybór pojedynczy oraz zbiorczy tj. „zaznacz wszystko") i wykonania określonej operacji jak na jednej wiadomości np. oznaczenie jako przeczytane, przeniesienie do folderu.
16) 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
17) Możliwość udostępniania przez użytkowników swoich folderów skrzynki pocztowej i ustanowienia poziomów uprawnień do zarządzania lub tylko do odczytu.
18) Możliwość definiowania przez użytkowników czarnych lub białych list e-mail.
19) Możliwość importu, eksportu konta, kalendarza, kontaktów przez administratora lub użytkownika (format pliku CSV, VCF lub inne równoważne).
20) Możliwość przejścia klienta webowego w tryb offline dla przeglądarek WWW tj. bez podłączenia do serwera poczty.
21) Możliwość włączenia podwójnego uwierzytelniania użytkowników przy dostępie do usługi web za pomocą dodatkowego kodu pin generowanego z poziomu aplikacji mobilnej w trybie offline.
22) Możliwość personalizacji wyglądu interfejsu webowego przez użytkownika poprzez dostępne w systemie pracy grupowej szablony wyglądu i kolorystyki, rodzaje czcionek oraz układy elementów widoku.
23) Możliwość edycji (już istniejących lub tworzenia nowych) dokumentów pakietu Office (min, dokument tekstowy, arkusz kalkulacyjny, prezentacja), zapisanych w folderach plikowych.
24) System musi zapewniać możliwość płynnego korzystania z usług (synchronizacja klientów z serwerem, dostęp poprzez Panel WWW) dla minimum jednoczesnych 300 użytkowników, w tym kalendarzy, poczty, zadań, kontaktów przy pomocy urządzeń mobilnych (w tym laptopy działające w systemach Microsoft Windows lub MacOS) pracujących na systemach iOS i Android.
25) Zapewnienie możliwości pracy off-line tj. pracy przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu.
26) Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem.
27) Możliwość bezpiecznego dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet - z dowolnego komputera lub urządzenia mobilnego, poprzez interfejs przeglądarkowy oraz z komputera przenośnego z poziomu standardowej aplikacji

klienckiej poczty, bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.

4.4. Dodatkowe funkcjonalności dot. kalendarzy i zadań

1) Planowanie spotkań i podglądu dostępności innych uczestników (wolny, zajęty).
2) Ustawianie przez użytkownika własnej informacji o dostępności.
3) Tworzenia spotkań cyklicznych oraz wyjątków do spotkań cyklicznych.
4) Funkcje rezerwacji zasobów (sala, wyposażenie, itp.) w ramach spotkania.
5) Wyszukiwanie dostępnych zasobów poprzez atrybuty (budynek, sala, piętro, itp.).
6) Możliwość włączenia alertu (pop-up) w związku ze zbliżającym się terminem.
7) Możliwość prezentacji kalendarza w co najmniej widokach: dzień, tydzień, miesiąc, dzień (godziny pracy), tydzień (godziny pracy), w każdym z widoków – możliwość tworzenia spotkania.
8) Możliwość konfiguracji godzin i dni roboczych.
9) Możliwość szybkiego akceptowania lub odrzucania terminu.
10) Możliwość włączenia lub wyłączenia przez użytkownika automatycznych powiadomień e-mail na temat spotkań.
11) Tworzenie przez użytkownika wielu kalendarzy w ramach jednego konta.
12) Wyświetlanie wielu kalendarzy nakładanych w tym samym miejscu/widoku w ramach dostępnych widoków – każdy kalendarz jest wyświetlany jest przez inny kolor; możliwość pracy na wielu kalendarzach w tym samym widoku.
13) Możliwość definiowania zadań tj. ustanowienia daty rozpoczęcia, priorytetu, śledzenia postępu i wykonania.
14) Możliwość dołączania załączników (plików) do poszczególnych zadań.

4.5. Dodatkowe funkcjonalności dot. pracy grupowej

1) Funkcjonalność planowania spotkań z możliwością zapraszania uczestników oraz zasobów (np. sala, rzutnik) wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń oraz możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
2) Możliwość udostępniania książek adresowych, zadań z możliwością definiowania poziomów dostępu do zadań, książek adresowych.
3) Możliwość oznaczenia terminów w kalendarzach jako publiczne lub prywatne oraz podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze z zachowaniem stopnia udostępnienia kalendarza.
4) Możliwość udostępniania kalendarzy dla innych użytkowników w trybach: tylko do odczytu, do edycji.
5) Możliwość współdzielenia zadań z użytkownikami wewnętrznymi i zewnętrznymi wraz z ustanowieniem odpowiednich uprawnień (odczyt, zapis).
6) Funkcjonalność udostępniania współdzielonych skrzynek pocztowych.
7) Obsługa list i grup dystrybucyjnych – możliwość definiowania dynamicznych grup dystrybucyjnych na podstawie stanowiska, działu, lokalizacji itp.
8) Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych użytkownika bez potrzeby wsparcia ze strony pracowników wydziału IT.
9) Możliwość zdefiniowania wielu domen pocztowych i prowadzenia w nich kont użytkowników.

4.6. Funkcjonalność klienta off-line

1) Możliwość współpracy z programem Microsoft Outlook w wersjach 2016, 2019, 2021 zapewniająca dwustronną synchronizację poczty, kontaktów i kalendarza między programem Microsoft Outlook, a serwerem Systemu BPF.
2) Możliwość przechowywania wiadomości w programie Microsoft Outlook w trybie offline.
3) Możliwość automatycznej konfiguracji i dostępu do globalnej książki adresowej pomiędzy programem Microsoft Outlook a serwerem Systemu BPF.
4) Możliwość bezpiecznego połączenia przez HTTPS, szyfrowanie całego ruchu między
5) programem Microsoft Outlook a serwerem Systemu BPF.
6) 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.
7) Możliwość udostępnienia folderu pocztowego innym użytkownikom systemu oraz podłączenia w swoim widoku udostępnionych przez innych użytkowników folderów pocztowych.
8) Możliwość synchronizacji zadań utworzonych w programie Microsoft Outlook.
9) Możliwość synchronizacji kontaktów utworzonych w programie Microsoft Outlook
10) Możliwość dodawania stopek adresowych i ich synchronizacja z serwerem.
11) Możliwość pobierania z serwera tylko nagłówka wiadomości.
12) Automatyczne wykrywanie stanu połączenia online/offline bez konieczności ingerencji użytkownika w zmianę statusu.
13) Możliwość automatycznej, dwukierunkowej synchronizacji kategorii (tagów) wiadomości między programem Microsoft Outlook a serwerem Systemu BPF.
14) Możliwość automatycznego opóźniania wysłania wiadomości ze skrzynki użytkownika
15) Możliwość ustawienia i synchronizacji z serwerem informacji o nieobecności.
16) Możliwość sprawdzenia pojemności skrzynki oraz jej zajętości na serwerze z poziomu programu Outlook.
17) Możliwość dodania pełnomocników, czyli osób, które mogą wysyłać pocztę „w imieniu” lub „jako” użytkownik. Synchronizacja tej informacji z serwerem.
18) 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).
19) Wsparcie mechanizmu podwójnej autentykacji 2FA uruchomionej na serwerze Systemu BPF dla Microsoft Outlook w wersjach 2016, 2019, 2021.

4.7. Zarządzanie i administracja Systemem BPF

1) Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk.
2) Definiowanie rozmiaru i ograniczeń (quot) 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 Systemu BPF za pomocą wbudowanych mechanizmów.
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) 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.
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 Systemu BPF.
12) Możliwość realizowania kopii /odzyskiwania pojedynczej skrzynki lub zestawu skrzynek w sposób pozwalający na zachowanie dostępności i ciągłości pracy.
13) Umożliwienie przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie - nawet w godzinach pracy biurowej bez zakłócenia pracy użytkowników.
14) Możliwość definiowania zasad przechowywania: wszystkich wiadomości, wiadomości śmieci, wiadomości do odzyskania oraz wiadomości usuniętych.
15) Możliwość włączenia funkcji odzyskiwania przez użytkownika usuniętych elementów, w określonym przez administratora systemu czasie.
16) Możliwość integracji procesu uwierzytelniania wieloskładnikowego np. z Google Authenticator.
17) Możliwość administracji systemem przez interfejs przeglądarkowy oraz z poziomu klasycznej linii komend (CLI).
18) Możliwość tworzenia i zarządzania wieloma domenami w ramach jednej instancji serwera.
19) Możliwość korzystania z różnych globalnych list adresowych dla każdej z domen.
20) Możliwość przyznania określonej przestrzeni dyskowej dla określonej domeny i konta, możliwość przeniesienia domeny.
21) Możliwość delegacji uprawnień administratora dla poszczególnych poddomen.
22) Możliwość przypisania użytkownikowi zastępczego adresu e-mail (aliasu).
23) Możliwość tworzenia grup dystrybucyjnych wiadomości e-mail.
24) Logowanie czynności administracyjnych oraz czynności polegających na dostępie do danych z innych skrzynek pocztowych przez użytkowników posiadających uprawnienia.
25) System BPF musi zapewnić możliwość rozszerzania funkcjonalności poprzez dodatkowe moduły - zarówno od strony interfejsu użytkownika, jak i administratora - frontend.
26) System BPF musi zapewnić możliwość rozszerzenia i pełnej integracji w warstwie serwerowej (backend), a moduły warstwy interfejsu użytkownika muszą mieć możliwość instalacji z poziomu panelu administratora.
27) Producent Systemu BPF musi zapewnić dokumentację tworzenia dodatkowych modułów rozszerzających zarówno warstwę frontend i backend.

5. Funkcje modułu archiwizacji skrzynek pocztowych.

1) Moduł musi zawierać funkcjonalność archiwizacji wiadomości oferujący możliwość wyszukiwania wiadomości po ich treści oraz załącznikach, sortowanie według zadanego klucza oraz konfigurowanie polityki retencji dla minimum 50 kont.
2) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi dostęp do wiadomości przechowywanych w archiwum za zgodą administratora systemu.
3) System powinien być wyposażony w mechanizmy nadrzędne, pozwalające na włączenie automatycznej archiwizacji wszystkich wiadomości wchodzących i wychodzących dla jednego lub wielu kont w liczbie j.w.
4) Mechanizm archiwizacji musi umożliwiać wyszukiwanie wiadomości e-mail w aktywnych i zarchiwizowanych skrzynkach pocztowych oraz kopiowanie wyników do określonej skrzynki pocztowej.

6. Funkcje modułu bezpiecznej obsługi wiadomości podejrzanych

1) Możliwość przesłania w konfiguracji wieloserwerowej „podejrzanej" wiadomości email w sposób zautomatyzowany z poziomu panelu WWW użytkownika tj. za pomocą dedykowanego przycisku, użytkownik może zgłosić wiadomość email zawierającą podejrzaną (wg. jego oceny) treść lub załączniki.
2) W momencie zaznaczenia podejrzanej wiadomości (na liście z wiadomościami) i naciśnięciu przycisku w panelu WWW wywołane zostaną akcje:
   - Skompresowanie oryginalnego e-maila (w formacie eml) do archiwum zip/7z z nadanym ustalonym hasłem np. w postaci aktualnej daty;
   - Do przesyłanej wiadomości poza spakowanym plikiem zostanie automatycznie dołączony podgląd treści wiadomości w formie pliku graficznego;
   - Automatyczne wysłanie wiadomości z załącznikiem na ustalony adres e-mail administratora Systemu BPF i wg. określonego szablonu (treść/temat wiadomości),
   - Równoczesne automatyczne przeniesienie oryginalnej wiadomości do folderu Spam po stronie zgłaszającego podejrzaną wiadomość użytkownika.
3) W panelu administracyjnym, administrator modułu ma możliwość ustawienia:
   - Adresu wysyłki, na którą są przekazywane podejrzane wiadomości;
   - Szablonu tematu i treści wiadomości.

7. Funkcjonalność modułu automatycznego szyfrowania załączników

1) Automatyczne szyfrowanie załączników:
   - System powinien automatycznie szyfrować załączniki wybranych wiadomości w formacie archiwum ZIP z hasłem.
   - Proces szyfrowania powinien działać w tle, bez konieczności ręcznego uruchamiania przez użytkownika na podstawie uprzednio zdefiniowanych reguł.
2) Elastyczność wyboru wiadomości do szyfrowania:
   - Możliwość zdefiniowania reguł, które wiadomości mają być objęte szyfrowaniem (np. na podstawie odbiorcy, treści, klasyfikacji lub rodzaju załącznika).
   - Opcja ręcznego wyboru przez nadawcę czy załącznik w danej wiadomości powinien być szyfrowany.
3) Zarządzanie hasłami:
   - Możliwość automatycznego generowania haseł zgodnie z polityką organizacji (np. długość, złożoność).
   - Możliwość ustawienia hasła ręcznie przez nadawcę w przypadku szczególnych wymagań.

4) Kompatybilność i formaty:
   - Tworzone archiwum ZIP powinno być zgodne z ogólnie przyjętymi standardami, aby można je było otworzyć na różnych platformach i systemach operacyjnych.
   - Obsługa szyfrowania całych załączników, niezależnie od ich formatu (PDF, Word, Excel, obrazy, itp.).
5) Integracja z serwerem pocztowym:
   - Rozwiązanie powinno być zintegrowane z serwerem pocztowym, umożliwiając automatyzację bez konieczności dodatkowych działań użytkownika.
   - Obsługa zarówno środowisk on-premises, jak i chmurowych (np. Microsoft 365, Google Workspace).
6) Polityki bezpieczeństwa:
   - Możliwość definiowania centralnych polityk dotyczących szyfrowania, np. wymuszania szyfrowania dla określonych grup odbiorców lub wiadomości zawierających wrażliwe dane.
   - Wsparcie dla zgodności z regulacjami, takimi jak RODO i innych.
7) Intuicyjność i prostota użytkowania:
   - Proces szyfrowania powinien być transparentny dla użytkownika końcowego, z możliwością prostego włączenia lub wyłączenia tej funkcji.
   - Informowanie odbiorcy w wiadomości o istnieniu zaszyfrowanego załącznika oraz sposobie uzyskania hasła.
8) Logowanie i audyt:
   - Funkcja rejestrowania działań związanych z szyfrowaniem załączników (kto, kiedy, jakie pliki zostały zaszyfrowane).
     Możliwość generowania raportów dla celów audytu lub monitorowania zgodności z politykami organizacyjnymi.

8. Moduł bezpieczeństwa poczty

1) Moduł w pełni skonfigurowany dla oferowanego Systemu BPF oraz z innymi rozwiązaniami takimi jak Zabbix, Forti Analyser oraz Gray LOG.
2) Moduł instalowany jako odrębna maszyna wirtualna w ramach infrastruktury IT Zamawiającego, korzystający z komercyjnych baz zabezpieczeń dla systemu poczty.
3) Przewidywane środowisko instalacji obejmuje wykorzystanie maszyny wirtualnie z przydzielonymi zasobami min. 2 vCPU oraz 5 GB RAM i zastosowania 4 wirtualnych kart sieciowych.
4) System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością odpowiadającą maksymalnemu ruchowi sieciowemu tj. min. 10 tys. wiadomości wychodzących i przychodzących na godzinę w szczycie.
5) Moduł musi zapewniać pracę w trybach typu: gateway oraz transparent.
6) Możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
7) Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
8) Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
9) Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
10) Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Protection).

11) Możliwość skanowania załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
12) Definiowanie komunikatów powiadomień w języku polskim.
13) Kontrola antywirusowa i ochrona przed malware powinna zapewniać:
    - Skanowanie antywirusowe wiadomości SMTP.
    - Kwarantannę dla zainfekowanych plików, w tym poprzez skanowanie załączników skompresowanych.
    - Blokowanie załączników w oparciu o typ pliku.
    - Ochronę typu wirus outbrake.
    - Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania rezultatu skanowania.
    - Możliwość definiowania różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u powinny obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje typu discard / reject, dostarczenie do innego serwera, powiadomienie administratora.
    - 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.
14) Kontrola antyspamowa co najmniej poprzez poniższe metody i funkcje filtrowania spamu:
    - Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
    - Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
    - Szczegółowa kontrola nagłówka wiadomości i analiza heurystyczna.
    - Współpraca z zewnętrznymi serwerami RBL, SURBL.
    - Kontrola w oparciu o Greylisting oraz SPF.
    - Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
    - Filtrowanie treści wiadomości i załączników.
    - Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
    - Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.
    - Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
    - Możliwość wykrywania i ochrony przed podszywaniem się (spoofing).
    - Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu.
15) Ochrona przed atakami na usługę poczty poprzez:
    - Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
    - Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu oraz maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
    - Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
    - Weryfikacja poprawności adresu e-mail nadawcy.
16) Logowanie, raportowanie oraz zarządzanie poprzez:
    - Logowanie do zewnętrznego serwera SYSLOG lub równoważnego.
    - Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.

- Logowanie informacji na temat spamu oraz niedozwolonych załączników.
- Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
- Możliwość analizy przebiegu sesji SMTP.
- Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
- Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
- Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
- System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
- Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

17) Aktualizacja sygnatur i dostęp do baz funkcji ochronnych producenta
    - Praca w oparciu o bazę spamu oraz url - uaktualniane w czasie rzeczywistym.
    - Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
    - Dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów oraz powinny one obejmować: kontrolę Antyspam, URL Filtering, kontrola antywirusową, ochrona typu Virus Outbrake, Sandbox producenta rozwiązania, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy od zakończenia wdrożenia.

9. Dokumentacja powykonawcza – minimalna zawartość

1) Opis architektury Systemu BPF i jego integracji z systemami Zamawiającego, przepływ informacji pomiędzy serwerami, wraz z adresacją IP oraz pełnionymi funkcjami.
2) Schemat logiczny topologii serwerów (z uwzględnieniem nazewnictwa oraz adresacji symbolicznej i numerycznej, zastosowanych protokołów sieciowych/komunikacyjnych).
3) Opis kluczowych parametrów konfiguracji serwerów i komponentów Systemu BPF.
4) Opis wykorzystania zasobów dyskowych (pamięci masowej), punktów montowania, wykorzystywanych protokołów.
5) Opis i schemat routingu poczty wchodzącej i wychodzącej.
6) Opis zastosowanych zabezpieczeń ruchu pocztowego w tym zabezpieczeń AV/AS skonfigurowanych w ramach modułu bezpieczeństwa poczty.
7) Opis zastosowanych zabezpieczeń serwerów i Systemu BPF.
8) Opis procedur diagnostyki, usuwania awarii, aktualizacji, kopii zapasowych, archiwizacji.
9) Zestawienie danych inwentarzowych Systemu – dostarczone licencje, wersje, daty aktywacji, uprawnienia zamawiającego – daty rozpoczęcia i zakończenia.

---------- KONIEC DOKUMENTU ----------