Załącznik nr 6

Szczegółowy opis przedmiotu zamówienia

**Zakup oprogramowania do zarządzania siecią komputerową, inwentaryzacji, zwiększenia bezpieczeństwa i cyfryzacji urzędu**

# **Część 1**

# **Program do monitorowania, zarządzania siecią komputerową i inwentaryzacji – licencja na 160 stanowisk**

## Wymagania:

1. Monitorowanie infrastruktury:
	1. Wykrywanie urządzeń w sieci poprzez skanowanie PING oraz ARPPING
	2. Monitorowanie serwerów WWW i adresów URL
	3. Monitorowanie czasu ładowania strony internetowej
	4. Obsługa szyfrowania SSL/TSL w powiadomieniach e-mail
	5. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP – monitorowanie wartości za pomocą nazw zmiennych oraz OID
	6. Obsługa komunikatów Syslog i pułapek SNMP oraz ewidencjonowanie odebranych z nich danych(obsługa obejmująca logi routerów jak i komputerów końcowych)
2. Monitoring routerów i przełączników:
	1. Zmiana stanu interfejsów sieciowych
	2. Ruchu sieciowego
	3. Podłączonych stacji roboczych
	4. Ruchu generowanego przez podłączone do portów stacje robocze
	5. Wyświetlanie statystyk takich jak: czas odpowiedzi urządzenia, czas ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status SNMP, ostrzeżenie o zdarzeniu na urządzeniu
	6. Wydajność systemów Windows:
		1. Obciążenie CPU
		2. Pamięci RAM
		3. Zajętość dysków
		4. Transfer sieciowy
3. Inwentaryzacja:
	1. Prezentacja szczegółów dotyczących sprzętu: model, procesor, pamięci, płyty głównej, napędów itp.
	2. Informacje o zainstalowanych aplikacjach z wyświetleniem licencji
	3. Informacje w zakresie zmian przeprowadzanych na stacjach roboczych wraz ze zmianą adresu IP
	4. Możliwość odczytania numeru seryjnego (klucza licencyjnego)
	5. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania
	6. Podgląd informacji o konfiguracji systemu np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników systemu, harmonogramu zadań
	7. Tworzenie list plików użytkowników z określonym rozszerzeniem i zdalnym ich usuwaniem
	8. Wskazywanie kont/osób uprawnionych do zasobów
	9. Oznaczanie statusów sprzętu, np. w użyciu, naprawie, zutylizowany
	10. Raportowanie inwentaryzacji
4. Obsługa użytkowników:
	1. Monitorowanie procesów wraz z informacją o uruchomieniu procesu na podwyższonych uprawnieniach
	2. Informacja o edytowanych przez użytkownika dokumentach
	3. Informacja o transferze sieciowym użytkownika (ruch lokalny i transfer internetowy generowany przez użytkownika
	4. Informacji o wydrukach użytkownika, wykorzystaniu drukarek
	5. Blokowanie stron internetowych i możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej
	6. Blokowanie ruchu na określonych portach TCP/IP
5. Pomoc zdalna:
	1. Podgląd pulpitu użytkownika wraz z możliwością przejęcia nad nim kontroli
	2. Powielenie ekranu podczas pomocy technicznej (użytkownik i administrator widzą ten sam ekran)
	3. Baza zgłoszeń problemów technicznych
	4. Czat umożliwiający komunikację miedzy użytkownikami i administratorami
	5. Zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, modyfikacji, aktywacji, edycji uprawnień.
	6. Dostęp do plików stacji roboczej
6. Ochrona danych przed wyciekiem
	1. Blokowanie urządzeń, interfejsów i nośników typu: USB, FireWire, gniazd kart pamięci, dysków itp.
	2. Blokowanie interfejsów bezprzewodowych takich jak: Wi-Fi, Bluetooth, IRDA
	3. Alarmowanie o zdarzeniach podłączania/odłączania urządzeń zewnętrznych z możliwością ograniczenia alarmów do nośników niezaufanych
	4. Autoryzowanie urządzeń firmowych: pendrive, dysk zewnętrzny
	5. Centralna autoryzacja podłączanych urządzeń dla całej sieci
	6. Audyt operacji na plikach na urządzeniach przenośnych
	7. Monitorowanie operacji na plikach stacji roboczych (tworzenie, edytowanie, usuwanie, kopiowanie)

Wdrożenie i wsparcie techniczne

1. Usługa wsparcia dla oprogramowania musi obowiązywać przez minimalny okres 12 miesięcy licząc od dnia wdrożenia usługi.

3. Oferta powinna zapewniać wdrożenie i przeszkolenie.

4. W ramach wsparcia Wykonawca zapewni:

a) bezpłatny dostęp do wszelkich aktualizacji oprogramowania, wydań uzupełniających oraz poprawek programistycznych przez okres minimum 12 miesięcy;

b) bezpłatny dostęp do telefonicznego i mailowego wsparcia technicznego dla oprogramowania przez okres 12 miesięcy w języku polskim;

c) Wykonawca zapewni przyjmowanie zgłoszeń telefonicznych w godzinach 7:00 do 16:00 w dni robocze;

d) świadczenie usług Service Desk poprzez udzielanie odpowiedzi na zapytania kierowane pocztą elektroniczną lub telefonicznie przez przedstawicieli Zamawiającego pod wskazany przez Wykonawcę adres lub numer telefonu w terminie nie dłuższym niż 1 dzień roboczy od dnia przekazania zapytania;

**Część 2**

**Program do zwiększenia bezpieczeństwa sieci komputerowej ESET – licencja na 160 stanowisk**

Eset Protect Advanced ON-PrEM – migracja licencji z ESET Endpoint Antivirus na 160 stanowisk (identyfikator publiczny : 33B-TC5-PHJ ważna do dnia 2024-03-04

Wdrożenie i wsparcie techniczne

1. Usługa wsparcia dla oprogramowania musi obowiązywać przez minimalny okres 12 miesięcy licząc od dnia wdrożenia usługi.

2. Oferta powinna zapewniać wdrożenie i przeszkolenie.

3. W ramach wsparcia Wykonawca zapewni:

a) bezpłatny dostęp do wszelkich aktualizacji oprogramowania, wydań uzupełniających oraz poprawek programistycznych przez okres minimum 12 miesięcy;

b) bezpłatny dostęp do telefonicznego i mailowego wsparcia technicznego dla oprogramowania przez okres 12 miesięcy w języku polskim;

c) Wykonawca zapewni przyjmowanie zgłoszeń telefonicznych w godzinach 7:00 do 16:00 w dni robocze;

d) świadczenie usług Service Desk poprzez udzielanie odpowiedzi na zapytania kierowane pocztą elektroniczną lub telefonicznie przez przedstawicieli Zamawiającego pod wskazany przez Wykonawcę adres lub numer telefonu w terminie nie dłuższym niż 1 dzień roboczy od dnia przekazania zapytania;

**Część 3**

**Program do elektronicznego zarządzania dokumentacją EZD licencja na 160 stanowisk**

Wymagania:

- system EZD musi być w pełni zgodny z obowiązującymi przepisami prawa administracyjnego w szczególności z obowiązującą Instrukcją Kancelaryjną.

- zapewniać poziom bezpieczeństwa dzięki logowaniu do systemu przy pomocy silnego klucza wykorzystującego algorytm szyfrowania SHA2 w wariancie SHA-512, podpisanego bezpiecznym certyfikatem. Certyfikaty generowane przez system dla każdego użytkownika

- aktualizacje systemu wykonywane bezpłatnie i automatycznie umieszczane na serwerze

- interfejs: prosty w obsłudze, graficzny, polskojęzyczny

- kompatybilny z platformami i systemami: Windows, Linux, iOS, macOS, Android i obsługiwany przez dowolną przeglądarkę internetową

- system ezd nie może pracować tylko na Windows Server oraz wykorzystywać licencje CAL

- system ma zapewniać automatyczną integrację ze skrzynką podawczą na EPUAP2, pobierać i wysyłać pliki bez konieczności wcześniejszego logowania się do skrzynki i mieć możliwość „masowej” wysyłki jednego pisma do wielu adresatów dokumentów elektronicznych przez ePUAP oraz automatycznie przypisywać UPP do konkretnej sprawy

-pobieranie i wysyłania tzw. „dużych plików" poprzez ePUAP2 bez konieczności wcześniejszego logowania się do skrzynki ePUAP2

- automatyczna integracja z interfejsem składania podpisu bezpośrednio z systemu profilem zaufanym lub możliwość składania podpisu podpisem kwalifikowanym w systemie Windows

- możliwość rejestracji korespondencji w rożnych budynkach i lokalizacjach poprzez sieć

Internet wraz z załącznikami.

- automatyczne numerowanie i asygnowanie przesyłek w postaci kodu kreskowego QR oraz tworzenie raportów i zestawień

- możliwość przeprowadzenia integracji dowolnego systemu dziedzinowego z system EZD

- moduł pocztowy zintegrowany z systemem Poczty Polskiej tzw. Elektronicznym Nadawcą Poczty Polskiej w pełni automatyzujący proces sporządzania, nadawania i wysyłania listów poleconych wraz z automatyczną weryfikacją terminów oraz statusów doręczeń (Śledzenie Przesyłek - "Tracking")

- znakowanie dokumentów i spraw unikalnymi sygnaturami wg schematu numeracji obowiązującego w jednostce,

- integracja systemu EZD z Platformą Elektronicznego Fakturowania (PEF) poprzez dowolnie wybranego Brokera

- wielopoziomowa dekretacja wpływającej korespondencji z możliwością niezależnego kierowania oryginałów dokumentów. Każda czynność związana z poszczególnym dokumentem, jest rejestrowana (historia obiegu)

- rejestracja poczty elektronicznej, faksów

- drukowanie pieczęci wpływu i sygnowanie korespondencji kodem kreskowym QR

- drukowanie potwierdzenia przyjęcia pisma dostarczonego osobiście przez interesanta

- gromadzenie bazy danych o nadawcach pism i kontrahentach

- ustalanie terminów rozpatrywania i załatwiania spraw związanych z pismem

- zestawianie statystyk i raportów dotyczących korespondencji przychodzącej oraz drukowanie tych raportów

- gromadzenie spraw w teczkach i podteczkach wg Jednolitego Rzeczowego Wykazu Akt i

udostępnianie zgodnie z uprawnieniami.

- mechanizmy dokonujące eksportu wybranych danych do Biuletynu Informacji Publicznej zgodnie z obowiązującymi standardami formatu danych oraz zapewnia otwarty interfejs integracji z dowolnym Systemem BIP.

- sprawdzanie stanu sprawy poprzez Internet

- dołączanie dowolnych dokumentów do akt sprawy: przesyłek przychodzących

i wychodzących, dokumentów wewnętrznych.

- śledzenie historii przebiegu sprawy wraz z jej metryką od chwili zarejestrowania jej w systemie oraz drogi obiegu dokumentów sprawy pomiędzy komórkami

organizacyjnymi i pracownikami

- możliwość rozbudowy systemu o jednostki podległe z wykorzystaniem serwera centralnego na którym będzie zainstalowany system EZD dla UM Chojnice

- po zakończeniu umowy system EZD przechodzi w stan „tylko do odczytu”, który umożliwia bezterminowo przeglądanie wszystkich wprowadzonych danych bez możliwości ich edycji oraz dodawania nowych.

Wdrożenie i wsparcie techniczne

1. Usługa wsparcia dla oprogramowania musi obowiązywać przez minimalny okres 12 miesięcy licząc od dnia wdrożenia usługi.

2. Oferta powinna zapewniać wdrożenie i przeszkolenie.

3. W ramach wsparcia Wykonawca zapewni:

a) bezpłatny dostęp do wszelkich aktualizacji oprogramowania, wydań uzupełniających oraz poprawek programistycznych przez okres minimum 12 miesięcy;

b) bezpłatny dostęp do telefonicznego i mailowego wsparcia technicznego dla oprogramowania przez okres 12 miesięcy w języku polskim;

c) Wykonawca zapewni przyjmowanie zgłoszeń telefonicznych w godzinach 7:00 do 16:00 w dni robocze;

d) świadczenie usług Service Desk poprzez udzielanie odpowiedzi na zapytania kierowane pocztą elektroniczną lub telefonicznie przez przedstawicieli Zamawiającego pod wskazany przez Wykonawcę adres lub numer telefonu w terminie nie dłuższym niż 1 dzień roboczy od dnia przekazania zapytania;

**Część 4**

#####

##### **Program do szyfrowania wiadomości email technologią END TO END i zabezpieczania poczty meilowej przed atakami**

##### **– licencja na 160 stanowisk**

Wymagania:

1. Oprogramowanie musi zapewnić:
	1. szyfrowanie algorytmem AES256 treści wiadomości,
	2. szyfrowanie algorytmem AES256 załączników,
	3. szyfrowanie algorytmem AES256 plików,
	4. szyfrowanie algorytmem AES256 katalogów,
	5. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego.
	6. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe.
	7. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego.
	8. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego.
	9. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0
	10. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki
	11. generowanie bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,
	12. opieczętowanie każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność,
	13. zabezpieczenie każdego emaila dedykowanym unikalnym hasłem,
	14. posiadanie wewnętrznej bazy haseł, która umożliwia:
		1. export haseł do pliku,
		2. import haseł z pliku
		3. generowanie ponownie haseł w bazie
	15. posiadanie wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym,
	16. posiadanie menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów,
	17. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,
	18. wykrywania fałszywych emaili - Antiphishing,
	19. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,
	20. wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,
	21. wykrywanie niebezpiecznych dokumentów MS Office,
	22. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,
	23. definiowanie alarmów informujących o niebezpiecznych mailach i załącznikach,
	24. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych.
	25. współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.
2. Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.
3. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.
4. Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.
5. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.

 Wdrożenie i wsparcie techniczne

1. Usługa wsparcia dla oprogramowania musi obowiązywać przez minimalny okres 12 miesięcy licząc od dnia wdrożenia usługi.

2. Oferta powinna zapewniać wdrożenie i przeszkolenie.

3. W ramach wsparcia Wykonawca zapewni:

a) bezpłatny dostęp do wszelkich aktualizacji oprogramowania, wydań uzupełniających oraz poprawek programistycznych przez okres minimum 12 miesięcy;

b) bezpłatny dostęp do telefonicznego i mailowego wsparcia technicznego dla Oprogramowania przez okres 12 miesięcy w języku polskim;

c) Wykonawca zapewni przyjmowanie zgłoszeń telefonicznych w godzinach 7:00 do 16:00 w dni robocze;

d) świadczenie usług Service Desk poprzez udzielanie odpowiedzi na zapytania kierowane pocztą elektroniczną lub telefonicznie przez przedstawicieli Zamawiającego pod wskazany przez Wykonawcę adres lub numer telefonu w terminie nie dłuższym niż 1 dzień roboczy od dnia przekazania zapytania;

1. Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne przez 2 lata.