Załącznik nr 1 - Specyfikacja systemu do ochrony poczty elektronicznej oraz szkolenie

I. Specyfikacja systemu do ochrony poczty elektronicznej

1. Wymagania ogólne

System ochrony poczty elektronicznej musi zapewniać kompleksową ochronę z zastosowaniem mechanizmów antyspam, antywirus oraz antyspyware, bez limitu licencyjnego na ilość chronionych kont użytkowników. System musi być dostarczony w postaci jednolitej platformy sprzętowej oraz 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)
3. Tryb serwera poczty

2. Parametry fizyczne oferowanego systemu

1. System musi być wyposażony w minimum 4 porty Gigabit Ethernet RJ,,45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB .
3. System musi posiadać wbudowany port konsoli szeregowej.
4. Obudowa urządzenia przystosowana do montażu w szafie RACK i o wysokości nie większej niż 1U
5. Zasilanie z sieci 230V/50Hz.

3. Funkcje serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.
W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, MAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSu, TIS 1,0, TLS 1.1 oraz TIS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail — z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3),
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość pobierania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

4. Funkcje systemu ochrony poczty

Oferowany system musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.

2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 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 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 wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail tub IMAP.
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.
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.

5. Kontrola antywirusowa i ochrona przed malware

W tym zakresie oferowany 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. Powinny one obejmować co najmniej: logowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

9. Ochronę typu virus 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) dostarczaniem oczyszczonych w ten sposób wiadomości.

6. Kontrola antyspamowa

Oferowany 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 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: phishing, malicious, hacking, adult content).
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-Ievel)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: łagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

7. Ochrona przed atakami na usługę poczty

Oferowany 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. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5, Weryfikacja poprawności adresu e-mail nadawcy,

8. Funkcie logowania i raportowania Oferowany system 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.

9. Funkcje pracy w trybie wysokiej dostępności (HA)

Oferowany system 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.

10. Aktualizacje sygnatur dost do baz spamu

Oferowany system 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.

11. Zarzadzanie

Oferowany system 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.

12. Certyfikaty

Oferowany system powinien posiadać co najmniej dwie z poniższych certyfikacji:
VBSpam, VBIOO rated, Common Criteria NDPP, Ftps 140-2 Certified.

13. Serwisy i licencje

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 12 miesięcy.

14. Gwarancja oraz wsparcie

Oferowany system musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

II. Szkolenie z oferowanego systemu

1. Wykonawca zorganizuje podstawowe szkolenie z obsługi i konfiguracji oferowanego systemu, obejmujące co najmniej następujący zakres:
   - scenariusze wdrożenia
   - tryby pracy urządzenia
   - podstawowa konfiguracja urządzenia
   - konfiguracja interfejsów sieciowych
   - generowanie raportów
   - chronione domeny pocztowe
   - potwierdzanie odbiorców
   - kwarantanna
   - zarządzanie pocztą użytkowników
   - aliasy pocztowe
   - polityki w oparciu o adres IP
   - polityki w oparciu o adres odbiorcy
   - metody antyspamowe
   - profile i techniki
   - wskazówki konfiguracyjne
   - reputacja nadawcy/odbiorcy
   - moduł antywirusowy
   - profile skanowania treści i załączników
   - warunki skanowania
   - ustawienia użytkownika dot. kwarantanny
   - raporty z kwarantanny
   - uwierzytelnienie poprzez SMTP
   - protokół SMTP over TLS
   - aliasy pocztowe
   - routing poczty

2. Szkolenie powinno być zorganizowane w formie warsztatów on-line w wymiarze minimum 4 godzin podzielonych maksymalnie na 2 dni szkoleniowe w terminie nieprzekraczającym 30 dni od dnia dostawy systemu do ochrony poczty elektronicznej.

3. Odbycie szkolenia powinno zostać potwierdzone imiennym certyfikatem ukończenia oznaczonym zgodnie zasadami dotyczącymi realizacji projektu lub z wykorzystaniem poniższego przykładu:

Załącznik nr 2 - Minimalne wymagania dotyczące punktów dostępowych sieci bezprzewodowej.

I. Minimalne wymagania

Typ punktu	Wewnętrzny AP
Technologia MU-MIMO	2x2
Certyfikat Wi-Fi Alliance	Tak
Dynamiczny wybór częstotliwości DFS	Tak (CE)
PoE	IEEE 802.3af
Ilość anten	4 wewnętrzne WiFi + 1 wewnętrzna BLE
Typ anten	Zysk 4 dBi dla 2.4 GHz, 5 dBi dla 5 GHz
Ilość nadajników	2 + 1 BLE
Częstotliwość nadajnika 1	2.4 GHz b/g/n (2x2:2 stream), 20/40 MHz (256 QAM)
Częstotliwość nadajnika 2	5 GHz a/n/ac (2x2:2 stream), 20/40/80 MHz (256 QAM)
Maksymalna przepustowość	nadajnik 1: do 400 Mbps nadajnik 2: do 867 Mbps
Maksymalna moc transmisji	2.4 GHz: 23 dBm / 200 mW (2 chains combined)* 5 GHz: 24 dBm / 251 mW (2 chains combined)*
Interfejs	1x 10/100/1000 Base-T RJ45
Uwierzytelnianie	WPA, WPA2, WPA3 z 802.1x lub klucz współdzielony, WEP, Web Captive Portal, MAC lista zabroniona i dozwolona
EAP	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Wspierane typy SSID	Local-Bridge, Tunnel, Mesh
802.11ac Wave 2 MU-MIMO	Tak
Transmit Beamforming (TxBF)	Tak
Low-Density Parity Check (LDPC) Encoding	Tak
Maximum Likelihood Demodulation (MLD)	Tak
Kensington Lock	Tak
Możliwa integracja z urządzeniem FortiGate wyposażonym w kontroler sieci bezprzewodowej	Tak

Maximum Ratio Combining (MRC)	Tak
Agregeacja ramek A-MPDU i A-MSDU	Tak

II. Szkolenie z oferowanego sprzętu

Wykonawca zorganizuje podstawowe szkolenie z obsługi i konfiguracji oferowanego systemu, obejmujące co najmniej następujący zakres:

- podstawowa konfiguracja dostarczonego urządzenia
- konfiguracja kontrolera sieci bezprzewodowej FortiGate
- konfiguracja profili
- konfiguracja uwierzytelniania i szyfrowania
- dostęp dla gości
- konfiguracja wielu bezprzewodowych identyfikatorów SSID

1. Szkolenie powinno być zorganizowane w formie warsztatów on-line w wymiarze minimum 4 godzin podzielonych maksymalnie na 2 dni szkoleniowe w terminie nieprzekraczającym 30 dni od dnia dostawy systemu do ochrony poczty elektronicznej.

2. Odbycie szkolenia powinno zostać potwierdzone imiennym certyfikatem ukończenia oznaczonym zgodnie zasadami dotyczącymi realizacji projektu lub z wykorzystaniem poniższego przykładu:

Załącznik nr 3 – Licencje do rozwiązania zapewniającego uwierzytelnianie dwuskładnikowe:

Nazwa produktu	Ilość
Fortinet - FortiTokenMobile	10 użytkowników

Załącznik nr 4 – Licencje do systemu do centralnego zarządzania wykonywaniem kopii zapasowych serwerów i stacji roboczych:

- Subskrypcje obowiązujące przez okres minimum 12 miesięcy powinny pozwalać na:
  - Kopię nielimitowanej ilości maszyn wirtualnych w obrębie 1 fizycznego serwera stanowiącego podstawę do wirtualizacji (Bez limitu socketów oraz procesorów)
  - Kopię 3 stacji roboczych (Windows)
  - Korzystanie z przestrzeni chmurowej dostarczanej bezpośrednio przez producenta, min 500GB.
- Wsparcie techniczne obowiązujące przez okres minimum 12 miesięcy:
  - Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,
  - Zapewnia dostęp do aktualizacji oprogramowania,
  - Dostępne online materiały samopomocowe w języku polskim,
  - Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,

Ogólne możliwości systemu do centralnego zarządzania wykonywaniem kopii zapasowych serwerów i stacji roboczych:

1. Oprogramowanie może być dostarczane w dwóch scenariuszach:
   - Cloud(Software as Service),
   - On-premise.
2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
3. Zgodność z RODO
4. Interfejs systemu dostępny jest w języku: polskim,
5. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
6. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych opartych o systemy:
   - Debian: 9+
   - Ubuntu: 16.04+
   - Fedora: 29+
   - centOS: 7+
   - RHEL: 6+
   - openSUSE: 15+
   - SUSE Enterprise Linux (SLES): 12 SP2+
   - Windows Client: 7, 8.1, 10 (1607+)
   - Windows Server: 2012 R2+,
7. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,

8. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),

Zarządzanie:
1. Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej,
2. Zarządzanie całym systemem poprzez dashboardy,
3. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
4. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
5. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
6. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
7. Monitorowanie postępu działania zadania,
8. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
9. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
10. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
11. System pozwala na klonowanie planów kopii zapasowych,
12. System umożliwia reset hasła administratora w przypadku jego utraty,
13. Oprogramowanie umożliwia definiowanie retencji według schematów:
    - GFS(Grandfather-Father-Son),
    - FIFO(First-In, First-Out).
14. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
15. Konta użytkowników mogą być tworzone poprzez import pliku CSV,
16. Oprogramowanie umożliwia tworzenie grup urządzeń,
17. Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
18. System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:

    - System Administrator,
    - Backup operator,
    - Restore operator,
    - Viewer.

Składowanie danych:
1. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,

2. System umożliwia składowanie danych:
   - Lokalnie: zasób SMB, NFS, ISCSI, S3, katalog zabezpieczonego urządzenia.
   - W chmurze: Amazon Web Service, magazyn zgodny z S3, dostarczanej przez producenta.
3. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
4. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
5. System umożliwia replikacje danych między magazynami.

Możliwości odtwarzania:
1. Odtwarzanie granularne:
   - Pojedynczych plików z kopii obrazu dysku,
2. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
   - Windows: 7+,
   - Windows Server: 2012 R2+,
3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
4. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
5. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
6. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
7. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
8. Odtwarzanie zasobów plikowych z prawami dostępu,
9. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
10. Odtwarzanie danych według harmonogramu,
11. Przywracanie danych z określonego urządzenia/użytkownika,
12. Przywracanie kopii z wybranego magazynu.
13. System posiada możliwość nieodwracalnego kasowania danych,

Backup:
1. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
   - Systemów operacyjnych:
     - Alpine 3.10+,
     - Debian: 9+,
     - Ubuntu: 16.04+,
     - Fedora: 29+,
     - centOS: 7+,

  - RHEL: 6+,
  - openSUSE: 15+,
  - SUSE Enterprise Linux(SLES): 12 SP2+,
  - macOS: 10.13+,
  - Windows: 7, 8.1, 10(1607+),11
  - Windows Server: 2012 R2+,
- Środowisk wirtualnych:
  - Hyper-V,
  - VMware: 6.7+.

- Repozytoriów GIT:
  - GitHub,
  - Bitbucket.

2. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
   - Baz danych:
     - Microsoft SQL,
     - MySQL,
     - PostgreSQL,
     - Firebird,
     - Dowolnych innych przez podpięcie skryptów pre/post.
3. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
   - 128 bit,
   - 192 bit,
   - 256 bit.
4. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
   - ZStandard,
   - LZ4.
5. Oprogramowanie umożliwia zarządzanie poziomem kompresji,
6. Wykonywanie kopii zapasowej otwartych plików(VSS),
7. System umożliwia uruchamianie skryptów przed i po backupie,
8. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
9. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
10. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
11. Backup plikowy,

12. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
13. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
14. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
15. Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.
16. Oprogramowanie pozwala na backup zaszyfrowanych partycji.
17. Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),
18. Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).

Załącznik nr 5 – Minimalne wymagania laptopów wraz z pakietem biurowym

Informacje ogólne	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. **W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.**
Ilość laptopów	7 sztuk
Pakiet oprogramowania biurowego	Microsoft Office 2021 PL dla Użytkowników Domowych i Małych Firm PL; licencja nieograniczona czasowo (z oprogramowaniem Word, Excel, Outlook, PowerPoint) lub inne równoważne, charakteryzujące się następującymi parametrami: • oprogramowanie musi zawierać: edytor tekstów, arkusz kalkulacyjny, program komunikacyjny zapewniający ujednolicone miejsce do zarządzania pocztą e-mail, kalendarzami, kontaktami, program do tworzenia prezentacji multimedialnych, • oprogramowanie będzie wykorzystywane na stacjach roboczych, których pracownicy współpracują i wymieniają informację z innymi zewnętrznymi podmiotami lub osobami, dlatego też musi zapewniać pełną kompatybilność oraz poprawną pracę z formatem plików pakietu Microsoft Office, • oprogramowanie musi być w pełni kompatybilne z aplikacjami Urzędu Gminy, w szczególności Systemem Elektronicznego Zarządzania Dokumentacją (EZD) firmy Comarch • dokumenty utworzone w programach pakietu MS Office (edytor tekstów, arkusz kalkulacyjny oraz program do tworzenia prezentacji) otwarty na zaoferowanym przez Wykonawcy programie musi poprawnie się uruchamiać, wydruk musi wyglądać identycznie bez jakiejkolwiek konieczności dodatkowej jego edycji oraz wszystkie funkcje muszą działać poprawnie a ich wynik musi być identyczny jak w przypadku programu z pakietu MS Office, bez konieczności reedycji otwartego dokumentu, • prawa licencyjne nie mogą ograniczać możliwości wykorzystania oprogramowania przez pracowników zamawiającego,

	• warunki licencji nie mogą ograniczać możliwości przeniesienia jej na inny komputer zamawiającego. • Licencjonowanie umożliwiające użytkowanie przez administrację rządową. • produkt musi być w nowy, wcześniej nie rejestrowany, fabrycznie zapakowany, • dopuszcza się zarówno wersję elektroniczną licencję (ESD) jak i „pudełkową" (BOX), • produkt musi pochodzić z legalnego źródła.
Ilość pakietów oprogramowania biurowego	7 sztuk
Ekran	• Matryca TFT, • Przekątna 15,6" z podświetleniem w technologii LED WVA • Rozdzielczość: FHD 1920x1080, 220nits.
Chipset	Dostosowany do zaoferowanego procesora.
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. Możliwość instalacji dwóch dysków twardych 1x M.2 oraz 1x 2.5.
Procesor	Procesor czterordzeniowy, osiągający w testach: PassMark CPU Mark wynik min. 10000 punktów według wyników ze strony https://www.cpubenchmark.net/ - **wynik w oferowanej konfiguracji należy załączyć do oferty.**
Pamięć operacyjna	Min 8GB z możliwością rozbudowy do 32GB, rodzaj pamięci min. DDR4, 2666MHz.
Dysk twardy	Min. 512GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 2 GB pamięci. Karta osiągająca w teście G3D Mark wynik min. 2500 pkt. wynik ze strony: https://www.videocardbenchmark.net/ - **załączyć do oferty.**
Audio/Video	• Wbudowana karta dźwiękowa, zgodna z HD Audio, • Wbudowane głośniki stereo, • Wbudowany mikrofon, • Kamera HD720p.
Karta sieciowa	Zintegrowana z płytą główną 10/100/1000 – RJ 45.
Porty/Złącza min	USB 2.0 - 1 szt.

	USB 3.2 Gen. 1 - 2 szt. HDMI 1.4 - 1 szt. Czytnik kart pamięci SD - 1 szt. RJ-45 (LAN) - 1 szt. Wyjście słuchawkowe/wejście mikrofonowe - 1 szt. DC-in (wejście zasilania) - 1 szt.
Klawiatura	Klawiatura podświetlana wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym.
WiFi	Wbudowana karta sieciowa, pracująca w standardzie min ac.
Bluetooth	Wbudowany moduł Bluetooth 5.1.
Bateria	Bateria – 3 komorowa, min 3400 mAh
Zasilacz	Zasilacz zewnętrzny max 65W.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego (TPM 2.0).
Waga	Waga urządzenia z baterią podstawową maksymalnie 1,9kg.
Oprogramowanie dodatkowe	Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : • upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, • możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: o o poprawkach i usprawnieniach dotyczących aktualizacji o dacie wydania ostatniej aktualizacji o priorytecie aktualizacji o zgodność z systemami operacyjnymi o jakiego komponentu sprzętu dotyczy aktualizacja • wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne • możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. • rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr),

	• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania), • dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera
System operacyjny	Windows 11 Professional 64 bit lub równoważny; System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: • Dostępne dwa rodzaje graficznego interfejsu użytkownika: o Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, o Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych • Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. • Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. • Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. • Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. • Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. • Wbudowany system pomocy w języku polskim. • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.

	• Klucz produktu przypisany do komputera aby przy ponownej reinstalacji systemu nie było konieczności wpisywania klucza. • Możliwość podłączenia do domeny Active Directory. W formularzu oferty trzeba podać nazwę oferowanego oprogramowania.
Gwarancja	3-letnia gwarancja
Wsparcie techniczne	Możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego.
Pozostałe	Sprzęt ma być fabrycznie nowy tj. nieużywany, nieuszkodzony, nieregenerowany, nieobciążony prawami osób lub podmiotów trzecich i wyprodukowany nie wcześniej niż na 24 miesiące przed terminem składania ofert oraz pochodzić z legalnego kanału sprzedaży producenta. Wszystkie sztuki laptopów muszą pochodzić od jednego producenta.

Załącznik nr 6 – Formularz ofertowy

FORMULARZ OFERTOWY

Dot. Zadania p.n.: Zakup i dostawa urządzeń, licencji oraz zabezpieczeń sieciowych.

ZP.271.3.30.2022.DJ

Nr referencyjny nadany sprawie przez Zamawiającego:

I. Zamawiający:

Gmina Radziejowice
ul. Kubickiego 10
96-325 Radziejowice
tel. 46-857 71 71

II. Wykonawca:

Niniejsza oferta zostaje złożona przez:

Nazwa Wykonawcy	Adres Wykonawcy

OSOBA UPRAWNIONA DO KONTAKTÓW:

Imię i nazwisko	
Adres	
Nr telefonu	
Adres e-mail	

III. Oferuję wykonanie zamówienia zgodnie z opisem przedmiotu zamówienia określonym w Zapytaniu ofertowym nr **ZP.271.3.30.2022.DJ**, oraz we wzorze umowy za następującą cenę:

Część I:	**Cena jednostkowa netto**	**Łącznie netto**	**Łącznie brutto**
Dostawa laptopów (7 sztuk)			
Dostawa oprogramowania biurowego (7 sztuk)			
Suma części I			
Część II:			
Dostawa punktów dostępowych (2 sztuk)			

zgodnie załącznikiem nr 2			
Przeprowadzenie szkolenia konfiguracja punktów dostępowych zgodnie załącznikiem nr 2			
System zabezpieczeń poczty elektronicznej (1 sztuka) zgodnie załącznikiem nr 1			
Szkolenie z systemu zabezpieczeń poczty elektronicznej zgodnie załącznikiem nr 1			
Dostarczenie licencji zabezpieczenia 2fa (10 sztuk) zgodnie załącznikiem nr 3			
Dostarczenie licencji na system kopii zapasowych, zgodnie załącznikiem nr 4			
Suma części II			

Cześć I:
netto …… zł plus …% VAT tj. brutto …… zł brutto.
Cena brutto słownie: ……zł

Cześć II:
netto …… zł plus …% VAT tj. brutto …… zł brutto.
Cena brutto słownie: ……zł

1. Oświadczamy, że proponowane przez nas produkty posiadają wymagane przez Zamawiającego parametry (lub lepsze), które określone zostały w opisie przedmiotu zamówienia znajdującym się w przesłanym zapytaniu ofertowym.
2. Zapoznałem się z opisem przedmiotu zamówienia oraz wzorem umowy i nie wnoszę do nich zastrzeżeń,
3. W razie wybrania niniejszej oferty jako najkorzystniejszej, zobowiązuję się do podpisania umowy w miejscu i w terminie określonym przez Zamawiającego,
4. Posiadam odpowiednią wiedzę i doświadczenie oraz posiadam odpowiednie kwalifikacje i uprawnienia pozwalające mi na wykonanie przedmiotu umowy oraz wykonam to zadanie zgodnie z obowiązującymi normami i przepisami prawa,
5. Wykonam zamówienie zgodnie z wymogami określonymi w zapytaniu ofertowym oraz wzorze umowy,
6. Podana cena zawiera wszystkie koszty związane z wykonaniem w/w zamówienia,
7. Oświadczam, iż zapoznałem/am się z klauzulą informacyjną z art. 13 RODO stosowaną przez Gminę Radziejowice zawartą w zapytaniu ofertowym w celu związanym z realizacją zamówienia.
8. Oświadczam, iż jestem świadom/a, że nie przysługuje mi na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania moich danych osobowych jest art. 6 ust. 1 lit. c RODO.

9. Oświadczam, że wypełniłem/am obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/am w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

_____

data i podpis *Wykonawcy/ pełnomocnika*

Umowa nr ……
zawarta w dniu ……r. w Radziejowicach

pomiędzy:
Gminą Radziejowice z siedzibą w Radziejowicach przy ul. Kubickiego 10, 96-325 Radziejowice
NIP 838-14-26-414, REGON 750148414, reprezentowaną przez:
Urszulę Ciężką–Wójta Gminy Radziejowice
przy kontrasygnacie Marleny Górniewskiej – Skarbnika Gminy Radziejowice
zwaną dalej w treści umowy „Zamawiającym”,
a firmą:
…….., reprezentowaną przez:
……- właściciela, zwanego dalej Wykonawcą.

Umowa niniejsza została zawarta w wyniku postępowania o udzielenie zamówienia publicznego o wartości szacunkowej nie przekraczającej kwoty określonej w art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019r. - Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 ze zm.), zgodnie z regulaminem udzielania zamówień o wartości szacunkowej nieprzekraczającej 130 000 złotych (zarządzenie nr 6/2020 Wójta Gminy Radziejowice ze zmianami z dnia 01.02.2021 r.).

§ 1.
Przedmiot umowy

1. Zamawiający powierza, a Wykonawca zobowiązuje się do realizacji przedmiotu umowy w:
   1) Część I obejmuje dostawę:
      a) laptopów – 7 sztuk,
      b) oprogramowania biurowego - 7 sztuk,
   2) Część II obejmuje dostawę:
      a) zabezpieczenia poczty elektronicznej wraz ze szkoleniem– 1 sztuka,
      b) punktów dostępowych - 2 sztuk wraz ze szkoleniem,
      c) licencji zabezpieczenia 2fa – 10 sztuk,
      d) licencje na system kopii zapasowych
2. Przedmiot umowy realizowany jest zgodnie z zapisami zapytania ofertowego nr ZP.271.3.30.2022.DJ z dnia 22.09.2022 r. wraz z załącznikami.
3. Wykonawca zobowiązuje się, że dostarczone urządzenia są fabrycznie nowe, dopuszczone do użytku, posiada odpowiednie atesty, certyfikaty, świadectwa jakości i spełniają wymogi norm określone obowiązującym prawem.
4. Wykonawca nie wprowadzi do realizacji przedmiotu Umowy zamienników i innych rozwiązań bez zgody Zamawiającego, wyrażonej w formie pisemnej lub za pośrednictwem poczty elektronicznej.
5. Wykonawca zapewni Zamawiającemu kompleksową obsługę, przy zachowaniu maksimum staranności i fachowości we wszystkich czynnościach związanych z dostawą.
6. Wykonawca dostarczy przedmiot umowy w siedzibie Zamawiającego: Urząd Gminy w Radziejowicach, ul. Kubickiego 10, 96-325 Radziejowice.

7. Potwierdzeniem odbioru przedmiotu umowy przez Zamawiającego będzie podpisany Protokół zdawczo-odbiorczego bezpośrednio po dokonaniu dostawy, zainstalowaniu i sprawdzeniu sprzętu.

§ 2.
Termin realizacji Umowy

Wykonawca zrealizuje przedmiot umowy, określonymi w §1 umowy w terminie 5 tygodni od dnia podpisania umowy

§ 3.
Wynagrodzenie

1. Za wykonanie przedmiotu umowy określonego w §1 umowy, Strony ustalają wynagrodzenie ryczałtowe w łącznej kwocie **brutto: …… zł**, w tym podatek VAT 23 % w wysokości……. W tym:
   Część I zamówienia:
   Część II zamówienia:
2. Zapłata wynagrodzenia należnego Wykonawcy dokonywana będzie na rachunek bankowy wskazany przez Wykonawcę na fakturze.
3. Zamawiający zastrzega sobie możliwość rozliczenia płatności wynikających z Umowy za pośrednictwem metody podzielonej płatności (ang. split payment) przewidzianego w przepisach ustawy o podatku od towarów i usług.
4. Wykonawca oświadcza, że rachunek bankowy wskazany w ust. 2 powyżej:
   1) Jest rachunkiem umożliwiającym płatność w ramach mechanizmu podzielonej płatności, o którym mowa w ust. 3 powyżej;
   2) Jest rachunkiem znajdującym się w elektronicznym wykazie podmiotów, prowadzonym od 1 września 2019 r. przez Szefa Krajowej Administracji Skarbowej, o którym mowa w ustawie o podatku od towarów i usług;
   3) W przypadku gdy wskazany przez Wykonawcę rachunek bankowy nie spełnia warunków określonych w pkt 1 i 2 powyżej, opóźnienie w dokonaniu płatności w terminie określonym w umowie, powstałe wskutek braku możliwości realizacji przez Zamawiającego płatności wynagrodzenia z zachowaniem mechanizmu podzielonej płatności, bądź dokonania płatności na rachunek objęty wykazem, nie stanowi dla wykonawcy podstawy do żądania od Zamawiającego jakichkolwiek odsetek/odszkodowań lub innych roszczeń z tytułu dokonania nieterminowej płatności.
5. Zapłata za fakturę VAT nastąpi w terminie do 14 dni od daty dostarczenia oryginału prawidłowo wystawionej faktury VAT Zamawiającemu.

§ 4.
Postanowienia końcowe

1. W sprawach nieuregulowanych postanowieniami Umowy zastosowanie mają przepisy Kodeksu cywilnego.
2. Umowę sporządzono w trzech jednakowo brzmiących egzemplarzach, jeden egzemplarz dla Wykonawcy i dwa dla Zamawiającego.

ZAMAWIAJACY **WYKONAWCA**