Załącznik nr 7

OPIS PRZEDMIOTU ZAMÓWIENIA

Wdrożenie systemu bezpiecznej poczty elektronicznej wraz z rozbudową macierzy dyskowej oraz doposażeniem szaf serwerowych w systemy zasilania awaryjnego Urzędu Gminy i Miasta w Miechowie

A. Wymagania techniczno - funkcjonalne opisu przedmiotu zamówienia na dostawę, montaż i konfigurację

Wzmocnienie poziomu bezpieczeństwa środowiska IT Urzędu Gminy i Miasta w Miechowie poprzez wdrożenie zaawansowanych narzędzi i mechanizmów szkoleniowych, programistycznych i sprzętowych – ETAP I

I. Zadanie 1 – dostawa, montaż i uruchomienie zasilaczy UPS o mocy znamionowej min. 3kVA (kod CPV 31154000-0).

Lp.	Nazwa Komponentu	Wymagane minimalne parametry
1.	Typ	Zasilacz bezprzerwowy, On-Line, podwójna konwersja, VFI SS 111, zgodny z PN-EN IEC 62040-3
2.	Zastosowanie	Sprzęt będzie wykorzystywany do awaryjnego zasilania szaf typu RACK z zainstalowanymi urządzeniami elektronicznymi (serwery, przełączniki, macierze dyskowe, centrale telefoniczne)
3.	Wielkość zamówienia	4 sztuki (komplety)
4.	Moc znamionowa	nie mniej niż 3000VA/ 3000W;
5.	konfiguracja faz	1:1
6.	Napięcie znamionowe	110V - 300V
7.	Częstotliwość znamionowa	50/60 Hz z autodetekcją
8.	Zniekształcenia harmoniczne	< 5%
9.	Zgodność z systemem zasilania	TN
10.	Napięcie wyjściowe, przebieg	230 V, fala sinusoidalna
11.	Zdolność przeciążeniowa - tryb pracy z sieci	100 ÷ 105 % praca ciągła 105 ÷ 125 % przełączenie na bypass po 5 min 125 ÷ 150 % przełączenie na bypass po 30 s > 150 % przełączenie na bypass po 500 ms
12.	Sprawność w trybie zasilania z sieci	>=90%
13.	Wbudowane filtry przeciwzakłóceniowe	RFI / EMI
14.	Czas przełączenia	zasilanie <-> akumulatory: 0 ms zasilanie <-> bypass : 5 ms
15.	Wbudowane zabezpieczenia	zwarciowe / przeciążeniowe / temperaturowe
16.	Alarmy	przeciążenie / praca z akumulatorów / niskie napięcie akumulatorów / awaria wentylatorów

17.	Akumulatory	akumulatory bezobsługowe VRLA/AGM, zapewniające czas autonomii co najmniej 5 minut dla pełnego obciążenia oraz co najmniej 20 minut dla połowy obciążenia. Dopuszcza się rozwiązanie wyposażone w zewnętrzy moduł baterii, przy założeniu, że wysokość rozwiązania nie przekroczy 6U.
18.	Rozbudowa pojemności zasilacza	Urządzenie ma mieć możliwość podłączenia co najmniej 2 zewnętrznych zestawów baterii.
19.	EMI	PN-EN IEC 62040-2 - kat. C2
20.	EMS	PN-EN 61000-4-2 / PN-EN IEC 61000-4-3 / PN-EN 61000-4-4 / PN-EN 61000-4-5
21.	Stopień ochrony (PN-EN 60529:2003)	IP20
22.	Temperatura pracy	0 °C ÷ 40 °C
23.	Wilgotność	0 ÷ 95 % (bez kondensacji)
24.	Obudowa	obudowa wraz z kompletem szyn montażowych, przystosowana do instalacji w standardowej szafie „RACK 19”
25.	Porty/ Złącza	USB/RS232/styk bezpotencjałowy/karta SNMP
26.	Obsługa systemów operacyjnych	MS Windows / Linux / Unix / MacOS
27.	Oprogramowanie	Dedykowane oprogramowanie do obsługi zasilacza działające pod kontrolą co najmniej Windows serwer 2019, wersja językowa polska lub angielska, wersja pełna nie wymagająca odnawiania subskrypcji (oprogramowanie należy dołączyć do oferowanego zasilacza)
28.	Niezawodność / jakość wytwarzania	Niezawodność i jakość zaoferowanego zasilacza UPS ma być potwierdzona certyfikatami (należy dołączyć do oferty): Certyfikat CE
29.	Warunki gwarancji	Co najmniej 12 miesięczna podstawowa gwarancja producenta (fabryczna) na zaoferowane zasilacze awaryjne oraz co najmniej 12 miesięczna gwarancja producenta (fabryczna) na baterie dołączone do zaoferowanych zasilaczy. Serwis urządzeń musi byś realizowany przez producenta zaoferowanych zasilaczy awaryjnych lub autoryzowanego partnera serwisowego producenta – Oferent zobowiązany jest, przed podpisaniem Umowy z Zamawiającym, dostarczyć Zamawiającemu dokumenty potwierdzające ten fakt. Serwis zaoferowanego zasilacza awaryjnego musi być realizowany zgodnie z wymaganiami normy ISO 9001:2015 – Oferent zobowiązany jest, przed podpisaniem Umowy z Zamawiającym, dostarczyć Zamawiającemu dokumenty potwierdzające, że serwis urządzeń będzie realizowany zgodnie z tą normą.

II. Zadanie 2.1 – dostawa, montaż i konfiguracja półki macierzy dyskowej - (kod CPV 30233141-1)

Lp.	Nazwa Komponentu	Wymagane Parametry
1.	Typ	Półka macierzy dyskowej
2.	Zastosowanie	Sprzęt będzie wykorzystany do rozbudowy posiadanej przez Zamawiającego macierzy dyskowej Dell PowerVault ME5012 ST: 35GVZQ3. Zamawiana półka macierzy dyskowej ma być wykorzystana do instalacji systemu bezpiecznej poczty elektronicznej składającego się z dedykowanej specjalistyczną zapory sieciowej nowej generacji do zabezpieczania korespondencji email oraz serwera poczty – zadanie 2.2 opisane w niniejszym OPZ.
3.	Wielkość zamówienia	1 sztuka
4.	Wyposażenie w dyski	Identyczne co do producenta, modelu, typu i pojemności jak obecnie zainstalowane w macierzy Zamawiającego - 8 x SAS SEAGATE ST1200MM0099 1.2. TB 10K 12 Gb/s, 4 x NLSAS SEAGATE ST4000NM017A 4 TB 7,2 K 12 Gb/s (dostarczone dyski muszą być dedykowane do pracy z oferowaną półką macierzy i muszą być na liście kompatybilności producenta oferowanej macierzy). Zamawiający dopuszcza inne dyski z zachowaniem zgodności co do pojemności oraz warunku pracy w obecnie skonfigurowanych pulach dyskowych i możliwości skonfigurowania wybranych dysków półki macierzy jako dyski „hot spare” dla obecnie skonfigurowanych pul dyskowych.
5.	Połączenie z macierzą Zamawiającego	Porty SAS 12 Gbps. Należy dostarczyć kable połączeniowe 2 x 12Gb HD Mini – SAS to Mini-SAS 0,5 m cable
6.	Obudowa	obudowa wraz z kompletem szyn montażowych, przystosowana do instalacji w standardowej szafie „RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje co najmniej 12 dysków 3.5”,
7.	Niezawodność / jakość wytwarzania	Niezawodność i jakość zaoferowanej półki macierzy dyskowej ma być potwierdzona certyfikatami (należy dołączyć do oferty): Certyfikat CE ISO 14001:2015 ISO 9001:2015
8.	Warunki gwarancji	Zamawiający wymaga aby przedmiot zamówienia był dostarczony z co najmniej 3 letnią gwarancją Producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Zamawiający wymaga możliwości zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga 36 miesięcznego okresu gwarancji na dzień dostawy zaoferowanej półki dyskowej do siedziby zamawiającego Serwis zaoferowanego urządzenia musi byś realizowany przez jego producenta lub autoryzowanego partnera serwisowego

		producenta – wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta. Oferent zobowiązany jest, przed podpisaniem Umowy z Zamawiającym, dostarczyć Zamawiającemu dokumenty potwierdzające ten fakt. Serwis zaoferowanego urządzenia musi być realizowany zgodnie z wymaganiami normy ISO 9001:2015 – Oferent zobowiązany jest, przed podpisaniem Umowy z Zamawiającym, dostarczyć Zamawiającemu dokumenty potwierdzający, że serwis urządzeń będzie realizowany zgodnie z tą normą. W przypadku awarii dysków twardych w okresie gwarancji, dyski pozostają u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu, o spełnieniu tego warunku.
9.	Wsparcie techniczne	Zamawiający wymaga aby dla zaoferowanego urządzenia była możliwość sprawdzenia statusu gwarancji poprzez stronę WWW jego producenta, podając identyfikator klienta lub model zaoferowanego urządzania lub jego numeru seryjnego lub jego unikalny numer serwisowy oraz oraz aby była możliwość pobierania uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji na zaoferowany
10.	Wymagania dodatkowe	1. Zamawiający wymaga aby zaoferowana półka macierzy dyskowej była fabrycznie nowa, nieużywana we wcześniejszych projektach i nie starsza niż 6 miesięcy licząc od daty jej produkcji. 2. Zamawiający wymaga aby zaoferowana półka macierzy dyskowej pochodziła z oficjalnego kanału sprzedaży producenta na rynek polski, co oznacza, że musi być sprzętem posiadającym stosowny pakiet usług gwarancyjnych i wsparcie techniczno-serwisowe kierowanego do użytkowników z obszaru Rzeczpospolitej Polskiej. 3. Zamawiający wymaga dostarczenia urządzenia z kompletnymi, wieczystymi, licencjami na załączone do półki macierzy dyskowej oprogramowanie, konieczne do zapewnienia jej pełnej funkcjonalności - jeżeli są wymagane – przez cały okres użytkowania urządzenia. Zamawiający nie dopuszcza urządzeń, których pełna funkcjonalność wymaga odnawiania czasowego licencji. 4. Dostarczoną półkę macierzy dyskowej należy dostarczyć do siedziby zamawiającego, zamontować w szafie rack wskazanej przez zamawiającego, połączyć z macierzą dyskową zamawiającego oraz skonfigurować i uruchomić wg wskazań zamawiającego.

Zadanie 2.2 – dostawa, montaż (instalacja) i konfiguracja zaawansowanego, bezpiecznego systemu poczty elektronicznej składającego się z dedykowanej, specjalistycznej zapory sieciowej nowej generacji i serwera pocztowego - (kod CPV 48811000-6).

Lp.	Nazwa Komponentu	Wymagane Parametry
1.	Typ	Oprogramowanie – maszyna wirtualna dla hiperwizora Hyper V
2.	Zastosowanie	Dedykowany system ochrony przed pełnym spektrum zagrożeń związanych z pocztą e-mail, takimi jak: phishing, oprogramowanie ransomware, ataki typu zero-day, ataki typu BEC, który pozwala zapobiegać tym zagrożeniom, wykrywać je i reagować na nie w czasie rzeczywistym wraz z serwerem poczty elektronicznej.
3.	Wielkość zamówienia	1 Licencja typu Perpetual umożliwiająca zarządzenie co najmniej 2TB przestrzenią dyskową i tworzenie nieograniczonej liczby kont pocztowych.
4.	Wymagania ogólne	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym w oparciu o hyperwizor Hyper-V. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
5.	Podstawowe funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 50 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania

		dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Ochrona przed wyciekiem informacji poufnej DLP (Data Loss Prevention). 18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
6.	Kontrola antywirusowa i ochrona przed malware	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików.

		3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbreak. 10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.
7.	Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.

		9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. 13. Ochrona typu outbreak. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. 16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level) 17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
8.	Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.
9.	Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach

		pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
10.	Aktualizacje sygnatur, dostęp do bazy spamu	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
11.	Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
12.	Wymagane certyfikaty	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: 1. VBSpam, VB100 rated, 2. Common Criteria NDPP, 3. FIPS 140-2 Certified.
13.	Serwisy i licencje	System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów na okres 36 miesięcy.. Powinny one obejmować następujące usługi: Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbreak, Sandbox w chmurze, ochrona typu URL Click Protect, Content Disarm & Reconstruction, Business Email Compromise.
14.	Gwarancja oraz wsparcie	System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
15.	Serwer pocztowy - zastosowanie	Zaawansowane narzędzie programistyczne do zarządzania pocztą elektroniczną, umożliwiające użytkownikom dostęp do swojej skrzynki pocztowej z dowolnego miejsca i urządzenia za pośrednictwem przeglądarki internetowej oraz integrujące funkcje wysyłania i odbierania wiadomości e-mail, zarządzania

		kalendarzem, kontaktami i zadaniami.
16.	Wielkość zamówienia	Licencja bezterminowa dla minimum 250 kont bez limitu pojemności (rozmiaru) skrzynki pocztowej
17.	Wymagania ogólne	System ma umożliwiać wysyłanie i odbiór wiadomości e-mail, synchronizację kalendarza, kontaktów i zadań z różnymi urządzeniami. Filtrowanie wiadomości, zarządzanie folderami i tworzenie reguł automatycznego sortowania wiadomości.
18.	Bezpieczeństwo	Zaoferowany system ma zapewniać wysoki poziom bezpieczeństwa danych poprzez wbudowane zaawansowane funkcje zabezpieczające, takie jak szyfrowanie SSL/TLS, filtrowanie antyspamowe i antywirusowe, oraz możliwość konfiguracji wielopoziomowych uprawnień dostępu.
19.	Integracja z innymi narzędziami programistycznymi	System ma umożliwiać integrację z narzędziami i aplikacjami firm trzecich, tj.: Microsoft Outlook, Apple iCal, Google Calendar w zakresie co najmniej synchronizacji kalendarza, kontaktów i zadań.
20.	Organizowanie skrzynki pocztowej	System ma umożliwiać łatwe organizowanie skrzynki pocztowej poprzez tworzenie folderów, przenoszenie wiadomości do odpowiednich kategorii, oznaczanie ich jako przeczytane lub nieprzeczytane, filtrowanie i stosowanie reguł automatycznego sortowania wiadomości.
21.	Kalendarz i kontakty	Zaoferowany system ma być wyposażony w funkcje kalendarza i kontaktów umożliwiające tworzenie wydarzeń, planowanie spotkań, ustawianie przypomnień, oraz zarządzanie listą kontaktów.
22.	Autoryzacja dwuskładnikowa	System ma obsługiwać autoryzację dwuskładnikową dostępu do konta pocztowego (oprócz hasła głównego system ma wymagać podania dodatkowego losowego zmiennego w czasie kodu).
23.	Kontrola dostępu do kont pocztowych	System ma umożliwiać administratorom kontrolowanie dostępu do kont użytkowników poprzez nadawanie uprawnień dla poszczególnych użytkowników, określając, które funkcje i zasoby są dostępne dla poszczególnych osób.
24.	Integracja z AD	System ma umożliwiać synchronizację użytkowników AD Microsoft z wykorzystaniem protokołu LDAP w zakresie tworzenia kont pocztowych użytkowników oraz ich uwierzytelniania w procesie logowania się do serwera pocztowego
25.	Obsługiwane protokoły	SMTP, POP3, IMAP, SMTPS, IMAPS, POP3S, XMPP, LDAP, LDAPS, LMTP, HTTP, HTTPS, MILTER, NG
26.	Wymagania dodatkowe	1. System serwera pocztowego należy dostarczyć w najnowszej jego wersji na dzień odbioru zaoferowanego systemu. 2. Zaoferowany system serwera pocztowego ma współpracować z opisanym powyżej dedykowanym systemem bezpieczeństwa poczty elektronicznej. 3. Zaoferowane systemy należy zainstalować w środowisku wirtualnym Zamawiającego pracującym pod kontrolą systemu Microsoft Hyper-V 2019. 4. Zamawiający wymaga aby wszystkie elementy zaoferowanego systemu bezpiecznej poczty były fabrycznie nowe, nieużywana we wcześniejszych projektach i nie starsza niż 6 miesięcy licząc od daty ich produkcji.

		5. Zamawiający wymaga aby wszystkie elementy zaoferowanego systemu bezpiecznej poczty pochodziły z oficjalnego kanału sprzedaży producenta na rynek polski, co oznacza, że wszystkie elementy zaoferowanego systemu bezpiecznej poczty mają posiadać stosowne pakiety usług gwarancyjnych i wsparcie techniczno-serwisowe kierowane1 do użytkowników z obszaru Rzeczpospolitej Polskiej.
27.	Szkolenia administratorów zaoferowanego systemu bezpiecznej poczty	Zamawiający wymaga przeprowadzenia dedykowanych, certyfikowanych przez producentów wszystkich zaoferowanych systemów bezpiecznej poczty szkoleń dla administratorów – 3 osoby. Szkolenia należy przeprowadzić poza siedziba zamawiającego, w terminie przed odbiorem systemu.
28.	Szklenia użytkowników serwera pocztowego	Zamawiający wymaga przeprowadzenia szkoleń dla użytkowników bezpiecznego serwera pocztowego – 80 osób. Szkolenia należy przeprowadzić w siedzibie zamawiającego. Szkolenia powinny objąć co najmniej tematykę: 1. praca w systemie - przegląd możliwości systemu, tworzenie wiadomości i narzędzia dodatkowe 2. praca z kalendarzami - tworzenie spotkań, dodawanie zasobów do spotkań, planowanie pracy z kalendarzami 3. udostępniania zasobów - zasady tworzenia i zarządzania elementami udostępnionymi w systemie poczty 4. praca z własnymi ustawieniami - autoresponder, ustawienia konta, import i eksport danych Czas szkolenia co najmniej 4 godziny zegarowe.

B. Wymagania dodatkowe

1. Do każdego zadania Wykonawca dostarczy dokumentację powdrożeniową w formie papierowej i elektronicznej na pendrive, która będzie zawierała: streszczenie zakresu wdrożenia i architektury systemu, topologię instalacji, rysunki (plany), nazewnictwo, adresację, konfigurację urządzeń, procedury administracyjne, kontakt do serwisu.

2. Do każdego zadania Wykonawca zapewni Zamawiającemu w okresie gwarancji bezpłatne wsparcie techniczne, w wymiarze nie mniejszym niż 36 godzin roboczych, realizowane przez inżynierów posiadających kwalifikacje uzyskane i autoryzowane przez producentów zaoferowanych rozwiązań, w reżimie 8/5 (w dni robocze w godz. 8.00 – 16.00). Wsparcie techniczne ma być świadczone zdalnie (telefonicznie lub poprzez e-mail), a w szczególnych przypadkach, gdy usunięcie zaistniałego problemu nie może być wykonane zdalnie, osobiście przez inżynierów Wykonawcy w siedzibie Zamawiającego. Zakres wsparcia technicznego ma uwzględniać prace administracyjne na życzenie Zleceniodawcy przy rekonfiguracji sprzętu i usług w istniejącym środowisku informatycznym w ramach posiadanych licencji.

3. Zamawiający wymaga dostarczenia urządzeń z kompletnymi licencjami koniecznymi do zapewnienia pełnej funkcjonalności - jeżeli są wymagane – przez cały okres użytkowania urządzeń. Zamawiający nie dopuszcza urządzeń, których pełna funkcjonalność wymaga odnawiania czasowego licencji.

4. Zamawiający wymaga aby zaoferowany sprzęt pochodził z oficjalnego kanału sprzedaży producenta na rynek polski, co oznacza, że musi być sprzętem posiadającym stosowny pakiet usług gwarancyjnych i wsparcie techniczno-serwisowe kierowanego do użytkowników z obszaru Rzeczpospolitej Polskiej oraz Zamawiający wymaga aby zaoferowane sprzęty i oprogramowanie były fabrycznie nowe, nieużywane we wcześniejszych projektach i nie starsze niż 6 miesięcy licząc od daty ich produkcji.

5. Zamawiający wymaga dostarczenia urządzeń z kompletnymi, wieczystymi, licencjami na załączone do zaoferowanych urządzeń oprogramowanie, konieczne do zapewnienia ich pełnej funkcjonalności - jeżeli są wymagane – przez cały okres użytkowania urządzeń. Zamawiający nie dopuszcza urządzeń, których pełna funkcjonalność wymaga odnawiania czasowego licencji.

6. Dostarczone urządzenia i oprogramowanie należy dostarczyć do siedziby Zamawiającego, zamontować w szafach rack lub środowisku wirtualnym wskazanych przez Zamawiającego oraz skonfigurować i uruchomić wg wskazań Zamawiającego.

D. Odbiór przedmiotu zamówienia oraz warunki płatności:

Gotowość do odbioru przedmiotu zamówienia należy zgłosić Zamawiającemu w formie pisemnej przed upływem terminu realizacji zamówienia zawartego w umowie.
Za dostarczony i odebrany protokolarnie przedmiot zamówienia Oferent wystawi fakturę VAT w rozbiciu na poszczególne zadania z uwzględnieniem liczby dostarczonego asortymentu w ramach zadania.

E. Formularz ofertowy:

Proszę uzupełnić poniższą Tabelę.

Rodzaj	**Producent / Typ / Numer katalogowy (bezwzględnie wymagane)**	**sztuk (kompletów, zestawów, licencji)**	**Spełnia wymagania SIWZ (TAK/NIE)**
Zadanie 1. Zasilacz UPS			TAK / NIE
Zadanie 2. Półka macierzy dyskowej			TAK/NIE
Zadanie 3. System bezpiecznej poczty elektronicznej			TAK / NIE

UWAGA: Do oferty proszę dołączyć specyfikację oferowanego sprzętu i oprogramowania (fotografie, opisy parametrów techniczno funkcjonalnych), wykresy, itp., pobraną z oficjalnej strony www jego producenta.

Z uwagi na zależność realizacji Zadania 3 od realizacji Zadania 2., zadania te należy realizować łącznie. Zadanie 1. może być realizowane samodzielnie.

F. Uwagi

Proszę aby w umowie nie zawierać zapisów o rękojmi dostawy. Wymagana jest tylko i wyłącznie gwarancja producenta.