**Załącznik nr 1 do Umowy**

**Szczegółowy opis przedmiotu zamówienia**

**na zakup oprogramowania zabezpieczającego pocztę elektroniczną w domenie podlaskie.eu oraz wrotapodlasia.pl wraz ze sprzętem wymaganym do jego uruchomienia**

1. **Przedmiot zamówienia**
	1. Przedmiotem zamówienia jest dostarczenie i wdrożenie przez Wykonawcę na rzecz Zamawiającego rozwiązania informatycznego obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej, wraz z narzędziami do wykrywania infekcji oraz sprzętem wymaganym do jego prawidłowego funkcjonowania, zwanego dalej łącznie Systemem.
	2. Wdrożenie obejmować będzie uruchomienie i konfigurację Systemu przez Wykonawcę, zgodnie z wymaganiami Zamawiającego w zakresie niezbędnym do poprawnego działania tego Systemu.
	3. W ramach przedmiotu zamówienia Wykonawca zobowiązuje się w szczególności:

a) wdrożyć, uruchomić i skonfigurować System;

b) przygotować i dostarczyć pełną dokumentację,

c) przeprowadzić autoryzowane szkolenie z wdrażanego systemu dla min. 4 osób,

d) udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu jako całości, jak i poszczególnych jego elementów dla 3050 kont email,

f) udzielić Zamawiającemu gwarancji na System, w tym gwarancji na oprogramowanie i sprzęt na okres 3 lat od dnia odbioru dostawy, potwierdzonej na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy oraz świadczyć w tym okresie usługi gwarancyjne zgodnie z SOPZ,

g) świadczyć wsparcie i asystę techniczną na System na okres 3 lat od dnia odbioru dostawy, potwierdzonej na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy.

h) dostarczyć sprzęt wymagany do prawidłowej i wydajnej pracy Systemu w okresie udzielonej gwarancji.

1. **Wymagania ogólne systemu:**
	1. oferowany System musi pochodzić tylko z oficjalnych kanałów dystrybucyjnych producentów modułów na terenie Unii Europejskiej;
	2. System musi stanowić jednolite środowisko programowe, działać bez konieczności stosowania dodatkowych elementów, nie będących standardową częścią oferowanego rozwiązania danego producenta;
	3. oferowane rozwiązanie ma stanowić jednolity i kompleksowy System, skalowalny i elastyczny w kontekście potencjalnej rozbudowy, tj. objęcia ochroną kolejnych użytkowników;
	4. oprogramowanie do ochrony poczty musi posiadać tylko jedną konsolę zarządzającą;
	5. oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization);
	6. oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization);
	7. Zamawiający wymaga, aby wszystkie elementy i moduły dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez producenta rozwiązania) na dzień wdrożenia Systemu;
	8. żaden z modułów i elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży;
	9. czynności związane z wdrożeniem i konfiguracją Systemu muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Zamawiającego.
2. **Wymagania jakościowe wsparcia i asysty technicznej:**
3. zapewnienie ciągłości działania Systemu;
4. niezwłoczne usuwanie awarii oraz usuwanie błędów zgłoszonych przez Zamawiającego w Systemie, zgodnie z czasem reakcji serwisowej opisanym w pkt 3.2.;
5. świadczenie asysty i wsparcia technicznego administratorom Systemu;
6. pomoc techniczna i merytoryczna administratorom Systemu przy rozwiązywaniu bieżących problemów związanych z funkcjonowaniem i korzystaniem z Systemu;
7. pomoc w zakresie korzystania z Systemu administratorom Systemu;
8. udzielanie wsparcia i asysty technicznej przez Wykonawcę niezależnie od stopnia udokumentowania Systemu;
9. wsparcie w zakresie optymalnego wykorzystania oraz dostosowania Systemu do potrzeb Zamawiającego, oraz wszelkich zmian definiowalnych elementów Systemu, wsparcie obejmuje wszystkie moduły i funkcje zakupione w ramach niniejszego postępowania przez Zamawiającego;
10. wsparcie w bieżącym optymalizowaniu konfiguracji Systemu uwzględniające potrzeby Zamawiającego;
11. pomoc w analizie i wyszukiwaniu informacji w logach systemowych;
12. wsparcie i asysta techniczna powinna być udzielona w sposób kompletny i uznany za wystarczający przez Zamawiającego.
	1. **Wykonawca obowiązany będzie w szczególności:**
13. świadczyć usługę wsparcia i asysty technicznej telefonicznie, e-mailowo, on-line lub poprzez zdalne połączenie z infrastrukturą Zamawiającego, za pośrednictwem imiennego konta założonego dla każdego z pracowników wskazanego przez Wykonawcę do realizacji usługi, aktywność pracowników jest logowana i monitorowana;
14. aktualizację i konfigurację Systemu do najnowszej dostępnej wersji przez Wykonawcę;
15. rozwiązywać zgłaszane i samodzielnie zaobserwowane problemy związane z działaniem i obsługą Systemu;
16. Wykonawca w ramach udzielonej gwarancji na wezwanie i w terminie uzgodnionym z Zamawiającym wprowadzi poprawki, usprawnienia i nowe wersje oprogramowania dla Systemu, udostępniane przez producentów wdrożonego Systemu;
17. w ramach udzielonej gwarancji Zamawiającemu przysługuje prawo do używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez producentów Systemu bez ponoszenia dodatkowych kosztów finansowych przez Zamawiającego. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Zamawiającemu;
18. przyjmować zgłoszenia dotyczące awarii, błędów, usterek i potrzeb wsparcia bądź aktualizacji:
	* telefonicznie – w dni robocze Zamawiającego, w godzinach od 7:30 do 15:30,
	* e-mailem lub poprzez system zgłaszania błędów– całodobowo, 24/5/365;
19. reagować na zgłoszenia w czasie zgodnym z wymaganiami podanymi poniżej w pkt 3.2;
20. weryfikować i zapewniać prawidłowe działanie Systemu po dokonanych przez siebie lub Zamawiającego naprawach i modyfikacjach;
21. aktualizować dokumentację zgodnie z wprowadzanymi modyfikacjami Systemu;
22. prowadzić statystyki i przekazywać raport serwisowy w zakresie udzielanego wsparcia i asysty technicznej do 5 dni roboczych po zakończeniu każdego kolejnego trzymiesięcznego okresu świadczenia gwarancji;
23. w uzgodnieniu z Wykonawcą dopuszcza wykorzystywanie systemu zgłaszania błędów dostarczonego przez Wykonawcę.
	1. **Klasyfikowanie, diagnozowanie oraz rozwiązywanie błędów zgłaszanych przez administratorów Systemu:**
		1. fakt wystąpienia błędu, oraz jego ewentualną charakterystykę, ocenia się zawsze w odniesieniu do ostatniej wersji opisu funkcjonalnego Systemu, uzgodnionej pomiędzy Zamawiającym a Wykonawcą;
		2. przez rozwiązanie błędu lub ostateczne rozwiązanie błędu, rozumie się wdrożenie działań, dzięki którym dany błąd przestaje występować podczas zgodnego z przeznaczeniem korzystania z funkcji Systemu;
		3. przez obejście błędu rozumie się przekazanie do wiadomości Zamawiającego lub administratora Systemu szczegółowego opisu działań, dzięki którym procedury użycia Systemu, będące normalnie pod wpływem danego błędu, mogą zostać przeprowadzone w sposób wykluczający powstanie lub wpływ tego błędu;
		4. w ramach udzielonej gwarancji, wsparcia i asysty technicznej, Wykonawca będzie realizował zgłoszenia serwisowe awarii Systemu w następujący sposób:
24. Awaria Krytyczna - wada skutkująca nieprawidłowym działaniem Systemu powodująca albo całkowity brak możliwości korzystania z Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas Reakcji: do 4 godzin od chwili zgłoszenia serwisowego przez Zamawiającego, Czas Naprawy: do 24 godzin od chwili zgłoszenia serwisowego przez Zamawiającego;
25. Awaria Niekrytyczna – wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej: Czas Reakcji: do 4 godzin od chwili zgłoszenia serwisowego przez Zamawiającego, Czas Naprawy: do 72 godzin od chwili zgłoszenia serwisowego przez Zamawiającego.

Zamawiający może zawiesić czas usunięcia Awarii Niekrytycznej na maksymalnie 40 dni kalendarzowych, jeśli zachodzi potrzeba wydania poprawki producenta do Systemu, zawieszenie odbywa się na wniosek Wykonawcy złożony w formie elektronicznej lub papierowej.

* + 1. przez reakcję rozumie się dowolny sposób komunikacji ze strony przedstawiciela Wykonawcy, potwierdzający przyjęcie zgłoszenia oraz rozpoczęcie działań diagnostycznych;
		2. gdy zgłoszenia dokonano poza godzinami pracy Zamawiającego, zgłoszenie traktowane jest jako przyjęte o godzinie 7:30 wraz z rozpoczęciem najbliższego dnia roboczego Zamawiającego (**nie dotyczy awarii krytycznych**);
		3. w wyjątkowych wypadkach, za zgodą Zamawiającego czas realizacji przywrócenia pełnej funkcjonalności Systemu (rozwiązanie lub obejście awarii) lub termin ostatecznego rozwiązania problemu, może zostać uzgodniony pomiędzy Wykonawcą i Zamawiającym i tym samym różnić się od wartości parametrów czasowych opisanych powyżej.
1. **Wymagania w zakresie dokumentacji:**
	1. Wykonawca w uzgodnieniu z zespołem odbiorowym opracuje i dostarczy następującą dokumentację projektową:
		1. Projekt Wdrożenia Systemu, który musi zawierać, w szczególności: opis funkcjonalny i techniczny Systemu, wykaz wymaganych elementów Systemu, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania Systemu jako całości, harmonogram wdrożenia;
		2. Dokumentację Testów Akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z Szczegółowym Opisem Przedmiotu Zamówienia. Testy akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez zespół odbiorowy na etapie odbioru dokumentacji projektowej;
		3. powyższa dokumentacja ma być dostarczona w ciągu 10 dni roboczych od dnia podpisania umowy.
	2. Wykonawca opracuje i dostarczy dokumentację powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w szczególności:
		1. procedury i instrukcje dotyczące instalacji, konfiguracji Systemu;
		2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa;
		3. instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa;
		4. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem zespołu odbiorowego;
		5. Zamawiający wymaga przygotowania przez Wykonawcę min. 20 procedur obsługi;
		6. termin dostarczenia dokumentacji, do dnia odbioru dostawy, potwierdzonej na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy.
	3. Dokumentacja powinna być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje producenta mogą być dostarczone w języku angielskim lub polskim.
	4. Zamawiający określi, czy dostarczana dokumentacja jest wystarczająca i w przypadku braków Wykonawca uzupełni dokumentację o wskazane przez Zamawiającego braki.
2. **Wymagania dotyczące szkoleń:**
	* 1. w ramach realizacji Przedmiotu Umowy Wykonawca zapewni uczestnictwo w autoryzowanych przez producenta szkoleniach w zakresie podstawowej i zaawansowanej konfiguracji oprogramowania do ochrony poczty elektronicznej, zakończone autoryzowanym egzaminem wiedzy co najmniej czterech pracowników Zamawiającego, w terminie zaakceptowanym przez Zamawiającego;
		2. Wykonawca dostarczy autoryzowane materiały szkoleniowe w języku polskim lub angielskim;
		3. w przypadku, gdy Wykonawca zaproponuje przeprowadzenie szkolenia poza miejscem realizacji umowy tj. poza siedzibą (miejscowością) Zamawiającego jest zobowiązany do zapewnienia dojazdu do tego miejsca, zakwaterowanie uczestników, ich wyżywienie oraz powrót;
		4. szkolenia z oprogramowania do ochrony poczty elektronicznej muszą być przeprowadzone w języku polskim na terenie RP;
		5. szkolenia z oprogramowania do ochrony poczty elektronicznej muszą zostać przeprowadzone i zakończone przed podpisaniem końcowego protokołu odbioru umowy;
		6. jeśli pracownik Zamawiającego nie będzie mógł uczestniczyć w szkoleniu, wówczas będzie mógł zamienić szkolenie na voucher/talon/grant do wykorzystania przez Zamawiającego w odpowiadającym mu terminie.
3. **Wymagania w zakresie wdrożenia:**
	1. przeprowadzenie analizy środowiska pocztowego Zamawiającego;
	2. przygotowanie koncepcji wdrożenia Systemu w zakresie poniższych punktów:
		1. ochrona w trybie inline (MTA) poczty przychodzącej obsługiwanej przez lokalny serwer Zimbra;
		2. ochrona w trybie inline (MTA) poczty wychodzącej obsługiwanej przez lokalny serwer Zimbra.
	3. Przygotowanie projektu technicznego obejmującego swoim zakresem co najmniej:
		1. schemat przepływu poczty przychodzącej oraz wychodzącej;
		2. opis konfiguracji przepływu poczty przychodzącej oraz wychodzącej (email routing);
		3. opis konfiguracji polityk bezpieczeństwa;
		4. opis konfiguracji kwarantanny oprogramowania do ochrony poczty elektronicznej;
		5. opis dostępu do spersonalizowanej kwarantanny użytkowników.
	4. Konfiguracja oprogramowania do ochrony poczty elektronicznej zgodnie z zaakceptowanym przez zespół odbiorowy projektem wdrożenia w zakresie:
		1. konfiguracji obsługiwanych przez System domen pocztowych;
		2. konfiguracji przepływu poczty przychodzącej oraz wychodzącej;
		3. konfiguracji weryfikacji połączeń przychodzących pod względem rekordów SPF, DKIM oraz DMARC;
		4. konfiguracji wpisów SPF, DKIM oraz DMARC Zamawiającego;
		5. konfiguracji polityk bezpieczeństwa;
		6. konfiguracji mechanizmów analizy wiadomości;
		7. konfiguracji funkcjonalności przepisywania adresów URL w wiadomościach;
		8. konfiguracji kwarantanny, uprawnień dla odbiorców oraz spersonalizowanego dostępu do kwarantanny dla użytkowników Zamawiającego.
	5. Asysta podczas rekonfiguracji ruchu pocztowego uwzględniającego oprogramowanie do ochrony poczty elektronicznej.
	6. Przeprowadzenie testów weryfikujących działanie oprogramowania do ochrony poczty elektronicznej pod względem:
		1. dla poczty przychodzącej: poprawnego dostarczania wiadomości do odbiorcy;
		2. dla poczty wychodzącej: poprawnego wysyłania wiadomości;
		3. poprawnej analizy procesowanych wiadomości przychodzących oraz wychodzących;
		4. poprawnego zatrzymywania zainfekowanych wiadomości w kwarantannie oraz poprawnego ich zwalniania z kwarantanny.
	7. Przygotowanie dokumentacji powdrożeniowej opisującej co najmniej punkty projektu technicznego oraz opis wszelkich wprowadzonych konfiguracji do Systemu.
	8. Miejsca realizacji przedmiotu Umowy: ul. Wyszyńskiego 1, 15-888 Białystok oraz ul. Poleska 89, 15-874 Białystok.
	9. Montaż urządzeń, dostarczanych przez Wykonawcę, w szafie RACK wskazanej przez Zamawiającego. Montaż urządzeń Systemu będzie polegał na instalacji w dwóch budynkach Zamawiającego, oddalonych od siebie w odległości ok. 1 km i połączonych ze sobą ciemnymi włóknami światłowodowymi.
	10. Wykonanie okablowania oraz podłączenie do istniejącej infrastruktury Zamawiającego.
	11. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Zamawiającego.
	12. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy, w zakresie dokumentacji projektowej, będzie odbiór dostawy potwierdzony na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy
	13. Potwierdzeniem prawidłowej realizacji Przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie dostarczony raport z przeprowadzonych Testów Akceptacyjnych oraz odbiór dostawy potwierdzony na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy.
4. **Opis funkcjonalny Oprogramowania do ochrony poczty:**
	1. Oprogramowanie musi umożliwić analizę wiadomości email zarówno przychodzących jak i  wychodzących.
	2. Oprogramowanie musi::
5. umożliwiać wdrożenie w trybach:
* inline – działanie jako MTA, będąc pośrednikiem w ruchu email do serwerów poczty;
* BCC – działanie na pasywnej kopii wiadomości email generowanej przez inny system pocztowy;
1. umożliwiać instalację zarówno jako pierwszy system ochrony poczty w środowisku Zamawiającego jak i na instalację pomiędzy innymi systemami bezpieczeństwa poczty;
2. obsługiwać wiele domen pocztowych;
3. umożliwiać oddzielną konfigurację wszystkich typów polityk dla różnych domen pocztowych;
4. umożliwiać akceptowanie połączeń przychodzących wyłącznie z podanych adresów IP;
5. umożliwiać weryfikację parametrów SPF, DKIM oraz DMARC nadawcy wiadomości;
6. umożliwiać podejmowanie określonych akcji w zależności od werdyktu weryfikacji parametrów SPF, DKIM oraz DMARC, co najmniej: automatyczna kwarantanna wiadomości, odrzucenie połączenia, modyfikacja tematu wiadomości oraz dodanie nagłówka;
7. umożliwiać konfigurację mechanizmu DKIM dla wiadomości wychodzących;
8. wykrywać zagrożenia w poczcie email bazując na sygnaturach;
9. wykrywać zagrożenia w poczcie email wykonując analizę dynamiczną nieznanych zagrożeń w odizolowanym środowisku typu sandbox bazującym na autorskich mechanizmach wirtualizacji (hypervisor). Nie może wykorzystywać to tego celu dostępnych rozwiązań takich jak VMware, MS Hyper-V czy VirtualBox.
	1. Oprogramowanie musi zapewnić wykrywanie zaawansowanych ataków przenoszonych w załącznikach do poczty oraz kontrolę adresów URL umieszczanych w treści wiadomości oraz analizę samej wiadomości, przy czym:
10. po wykryciu wcześniej znanego, szkodliwego adresu URL musi być możliwe wygenerowanie alertu i umieszczenie wiadomości w kwarantannie;
11. po wykryciu nieznanego wcześniej adresu URL prowadzącego do pliku (co najmniej PDF, ZIP, EXE, DOC/DOCX) musi być możliwe automatyczne nawiązanie połączenia do Internetu przez oprogramowanie, pobranie pliku i przeanalizowanie go, a następnie w razie wykrycia zagrożenia, wygenerowanie alertu i zapisanie wiadomości email w kwarantannie.
	1. Oprogramowanie musi rozpoznawać i wyodrębniać malware oraz inne szkodliwe oprogramowanie w załącznikach do poczty niezależnie od użytego rozszerzenia pliku.
	2. Oprogramowanie musi umożliwiać wykorzystanie reguł, stworzonych samodzielnie przez Zamawiającego, opisujących cechy podejrzanych obiektów w formacie YARA.
	3. Oprogramowanie musi posiadać dodatkowe mechanizmy chroniące pocztę email Zamawiającego przed atakami:
12. phishing/spear phishing - podszywanie się pod inną organizację lub osobę w celu wyłudzenia m.in. danych uwierzytelniających);
13. impersonation (CEO fraud) - kradzieży informacji lub wywierania wpływu na podejmowane decyzje, w wyniku podszywania się pod osoby będące członkami kadry zarządzającej;
14. infekcją kodu JavaScript, VBScript;
15. spywre/adware - niebezpieczne aplikacje, odnośniki URL lub załączniki będące częścią ataku.
	1. Oprogramowanie musi posiadać mechanizmy analizujące wiadomości email pod kątem spamu, newsletterów oraz ataków typu APT.
	2. Oprogramowanie musi umożliwiać deszyfrację załączników przesyłanych przez pocztę email Zamawiającego przy użyciu listy najczęściej używanych haseł lub inteligentnego wyszukiwania haseł w treści maila.
	3. Oprogramowanie musi umożliwiać deszyfrację załączników w oparciu o hasło odczytane z obrazu graficznego (OCR) przesłanego w tej samej wiadomości.
	4. Oprogramowanie musi posiadać środowiska wirtualne służące do analizy zagrożeń co najmniej w systemach operacyjnych: Windows 7, Windows 10, Windows 11, MacOS i Linux. Maszyny wirtualne muszą być aktualizowane przez producenta oraz nie mogą wymagać posiadania dodatkowych licencji przez Zamawiającego.
	5. Oprogramowanie musi wykonywać analizę dynamiczną równocześnie w różnych wersjach systemów operacyjnych, różnych aplikacjach i różnych ich wersjach.
	6. Rozwiązanie musi analizować co najmniej następujące rodzaje plików:
16. rozszerzenia używane przez pakiet OFFICE, np. DOC/DOCX, XLS/XLSX, PPT/PPTX;
17. pliki wykonywalne, np. EXE, DLL;
18. inne, np. CHM, RAR, ACE, SCR, PDF, PUB, ZIP, MP3, 7Z, BZ, GZ, JAR, MHT, RTF, CAB.
	1. Oprogramowanie musi zapewniać dostęp do sekwencyjnego (krok po kroku) zapisu zmian wykonywanych przez załącznik w środowisku wirtualnym co najmniej w rejestrze, procesach, systemie plików, sposobie startu systemu, próby nawiązania połączenia sieciowego (wraz z zapisem tych prób w postaci plików PCAP dostępnych w GUI Oprogramowania) oraz umożliwiać pobranie artefaktów z przeprowadzonej analizy co najmniej w zakresie analizowanej próbki.
	2. Oprogramowanie musi posiadać mechanizm do wykrywania podszycia się pod inną osobę (na poziomie adresu email i wyświetlanej nazwy użytkownika oraz adresu email nadawcy i pola reply to).
	3. Oprogramowanie musi posiadać dodatkowy mechanizm wykrywania zdarzeń tak zwanych "commodity malware", takich jak zaszyfrowane dokumenty, pliki wykonywalne, pliki z załączonymi obiektami, nietypowe rozszerzenia plików, formularz HTTP\_request, wykorzystanie MagicBytes, przekierowania HTML w załączniku. Zdarzenia te powinny być konfigurowalne jako alert lub automatyczna kwarantanna.
	4. Oprogramowanie musi posiadać dodatkowych mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:
	5. skrypty przesyłane w wiadomości email;
	6. pliki wykonywalne przesyłane w załączniku lub URL;
	7. dokumentów MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym;
	8. nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO;
	9. wiadomości email ze skróconymi linkami (tiny URL);
	10. dokumentów MS OFFICE z flash;
	11. plików JAR;
	12. haseł przesyłanych w treści wiadomości HTTP request;
	13. zaszyfrowanych plików PDF;
	14. pliki typu wygaszacz ekranu;
	15. nieznanych plików konfiguracyjnych .SettingContent-ms.
	16. Oprogramowanie musi mieć możliwość przepisania nieznanych adresów URL w przesyłanej wiadomości, tak aby pomimo kliknięcia, użytkownik nie był przekierowany do potencjalnie złośliwej treści, a do strony producenta informującej (w języku polskim) o zablokowaniu tej komunikacji.
	17. Oprogramowanie musi posiadać mechanizm ekstrakcji (rozpoznawania) adresów URL z załączników przesyłanych w wiadomości email i możliwość detonowania ich w środowisku wirtualnym w przypadku pliku zlokalizowanego w URL.
	18. Oprogramowanie musi posiadać możliwość automatycznego generowania "screenshotów" stron phishingowych w przypadku wykrytego alertu.
	19. Oprogramowanie musi umożliwiać konfigurację reguł bazujących na wyrażeniach regularnych w celu modyfikacji ochrony w zakresie: adresu e-mail nadawcy, domeny nadawcy, adresu IP nadawcy, kraju nadawcy, adresu e-mail odbiorcy, treści wiadomości i jej tytułu (zarówno whitelisty jak i blacklisty).
	20. Oprogramowanie musi umożliwiać konfigurację reguł bazujących na wystąpieniu konkretnego nagłówka wiadomości oraz jego wartości i podejmować wskazaną akcję.
	21. Oprogramowanie musi dla punktów 7.20 oraz 7.21 umożliwiać podejmowanie wskazanych akcji w zakresie co najmniej: przeniesienie do kwarantanny, dostarczenie, utworzenie i wysłanie BCC, przesłanie na inny serwer pocztowy, zmodyfikowanie tytułu oraz dopisanie wskazanego nagłówka wraz z jego wartością. Niniejsze reguły muszą umożliwiać stosowanie wyjątków oraz stosowania kilku akcji jednocześnie.
	22. Oprogramowanie musi mieć zaimplementowany mechanizm wyszukiwania analizowanych wiadomości pocztowych zawierający filtry wyszukujące co najmniej przy użyciu: adresu email odbiorcy, adresu email nadawcy, adresu IP nadawcy, tematu wiadomości, nazwy załącznika, MD5 oraz SHA256 załącznika, werdyktu analizy z uwzględnieniem mechanizmów, które wygenerowały ewentualny alert (np. SPAM, AV, custom rules). Niniejszy mechanizm musi umożliwiać wyszukiwanie wiadomości co najmniej do 30 dni wstecz.
	23. Oprogramowanie musi analizować wiadomości email nawet po ich dostarczeniu i alertować o możliwej podmianie zawartości URL na złośliwą (analiza wsteczna).
	24. Oprogramowanie musi udostępniać spersonalizowaną dla każdego odbiorcy kwarantannę.
	25. Oprogramowanie musi umożliwiać precyzowanie uprawnień dla odbiorców wiadomości do zwalniania zablokowanych przez oprogramowanie wiadomości z jego spersonalizowanej kwarantanny w zależności od wykrytego zagrożenia.
	26. Oprogramowanie musi dostarczać do odbiorców powiadomienia mailowe z listą wiadomości znajdujących się w jego spersonalizowanej kwarantannie. Oprogramowanie musi mieć możliwość sprecyzowania częstotliwości dostarczania powiadomień oraz konfiguracji dostarczanej formatki.
	27. Oprogramowanie musi umożliwiać wysyłanie alertów o zdarzeniach poprzez protokoły SMTP oraz RSYSLOG.
	28. Oprogramowanie musi umożliwiać administratorom systemu pobranie wiadomości, która została zablokowana, jej wyświetlenie zarówno w formie sparsowanej, jak i tekstowo z uwzględnieniem jej nagłówków.
	29. Oprogramowanie musi umożliwić ręczne zwalnianie zablokowanych wiadomości z kwarantanny przez administratorów systemu.
	30. Oprogramowanie musi umożliwiać tworzenie dedykowanych pulpitów w GUI rozwiązania z możliwością dostosowania wyświetlanych informacji.
	31. Oprogramowanie musi umożliwiać generowanie raportów zawierających co najmniej:
	32. statystyki wykrytych alertów z rozbiciem na kategorie zagrożenia (co najmniej spam, impersonation, viruses, itp.);
	33. statystyki przeanalizowanych wiadomości email;
	34. statystyki najpopularniejszych adresów email oraz adresów IP nadawców oraz adresów email odbiorców;
	35. statystyki formatów przeanalizowanych załączników;
	36. powyższe statystyki powinny umożliwiać filtrowanie pod względem podłączonych do oprogramowania domen pocztowych.
	37. Raporty muszą mieć możliwość eksportu do formatu CSV lub PDF wraz z możliwością ustalenia okresu czasu dla generowanego raportu (co najmniej ostatnie 24 godziny, ostatni 7 dni, ostatnie 30 dni).
	38. Interfejs oprogramowania musi być w języku polskim lub angielskim.
	39. Dostęp do oprogramowania musi być zabezpieczone kryptograficznie poprzez szyfrowanie komunikacji.
	40. Oprogramowanie musi pozwalać na zdefiniowanie wielu administratorów o różnych poziomach uprawnień.
19. **Opis sprzętu:**
	1. Sprzęt musi zostać dostarczony w postaci fizycznego appliance pracującego w klastrze niezawodnościowym skonfigurowanym przez Wykonawcę.
	2. Dostarczony sprzęt musi zapewniać prawidłową i wydajną pracę oprogramowania do ochrony poczty.
	3. Poszczególne wymagania i parametry muszą być zrealizowane dla każdego z urządzeń fizycznych, tak aby wskazane parametry wydajnościowe zostały zachowane dla każdego datacenter w razie awarii lub niedostępności pojedynczego węzła klastra.
	4. Wszystkie dostarczane urządzenia Systemu muszą być w tej samej konfiguracji i wersji.
	5. Dostarczony sprzęt musi być fabrycznie nowy, aktualnie obecne w linii produktowej producenta i jednocześnie nie może znajdować się na liście „end-of-sale” oraz „end-of-support” producenta
	6. Sprzęt musi pochodzić z autoryzowanego kanału sprzedaży/dystrybucji producenta.
	7. Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane i wolne od wad fizycznych, w szczególności bez wad zmniejszających jego wartość lub użyteczność wynikającą z jego przeznaczenia.
	8. Sprzęt musi posiadać dołączone niezbędne instrukcje i materiały dotyczące użytkowania w języku polskim lub angielskim.
	9. Sprzęt musi posiadać trwałe oznaczenia zawierające: nazwę producenta, typ, oznakowanie CE, numer fabryczny (o ile są przewidziane przez producenta).
	10. Sprzęt musi być kompatybilny i możliwy do wdrożenia w infrastrukturze teleinformatycznej Zamawiającego, a Wykonawca oświadcza, że zapoznał się z wykorzystywaną przez Zamawiającego technologią, w tym używanym sprzętem, oprogramowaniem, doprowadzonym zasilaniem, zabezpieczeniami, architekturą serwerową oraz sieciową, systemami operacyjnymi niezbędnymi do wykonania umowy, oraz że przedmiot umowy będzie prawidłowo funkcjonować w zakresie, w jakim to konieczne do realizacji przedmiotu umowy w kooperacji ze sprzętem i oprogramowaniem Zamawiającego przy uwzględnieniu zabezpieczeń wykorzystywanych przez Zamawiającego.
	11. Sprzęt musi być dedykowany przez producenta do montażu w 19” szafie RACK Zamawiającego.
20. **Licencje i subskrypcje**
	1. W ramach postępowania muszą zostać dostarczone subskrypcje na okres 36 miesięcy od

dnia odbioru dostawy, potwierdzonej na podstawie sporządzonego zgodnie z wzorem załącznika nr 3 do Umowy.

* 1. Licencje na System nie mogą mieć ograniczeń czasowych (licencje wieczyste) z zastrzeżeniem, że nie dotyczy to licencji subskrypcyjnych, o których mowa powyżej.
	2. System musi być dostarczony z wszelkimi licencjami wymaganymi do prawidłowego działania Systemu jako całości, jak i poszczególnych jego elementów.

…………………………………………………….