

UWAGA!

Niezłożenie formularza zgodności wraz z ofertą/złożenie nie podpisanego formularza zgodności stosownym podpisem elektronicznym - tj. kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym - spowoduje odrzucenie oferty Wykonawcy na podstawie art. 226 ust. 1 pkt 5) ustawy Pzp.

FORMULARZ ZGODNOŚCI

(matryca spełnienia wymagań) — Zakup systemu bezpieczeństwa poczty elektronicznej wraz z rocznym wsparciem technicznym producenta

Lp.	Oferowany produkt – nazwa *
1.	

* podać nazwę oferowanego produktu

Instrukcja wypełnienia

Formularz zgodności należy złożyć wraz z ofertą. Formularz zgodności potwierdza spełnienie wymagań minimalnych określonych w Sekcji V OPZ.

Dla każdego wymagania należy wpisać w kolumnie „Spełnia (TAK/NIE)” wyraz TAK albo NIE. Wpisanie „NIE” albo pozostawienie pola pustego oznacza niespełnienie wymagania i skutkuje uznaniem, że oferta nie spełnia wymagań Zamawiającego i spowoduje odrzucenie oferty Wykonawcy.

Część A. Wymagania ogólne (Sekcja IV OPZ)

Wykonawca potwierdza spełnienie każdego z poniższych wymagań ogólnych dotyczących realizacji zamówienia, wpisując TAK albo NIE. Wpisanie „NIE” albo pozostawienie pola pustego oznacza niespełnienie wymagania.

Lp.	Wymaganie ogólne	Spełnia (TAK/NIE)
1	Rozwiązanie musi obsługiwać pełną liczbę 4 500 licencjonowanych użytkowników bez pogorszenia parametrów wydajnościowych i bez dodatkowych, nieuwzględnionych w ofercie kosztów w okresie obowiązywania umowy.	
2	Subskrypcja licencji oraz wsparcie producenta muszą obejmować nieprzerwany okres 12 miesięcy, liczony od dnia odbioru wdrożenia (lub innego dnia wskazanego w umowie).	
3	Wszystkie funkcjonalności wymagane w Sekcji V muszą być dostępne w ramach oferowanej licencji, bez konieczności dokupowania dodatkowych modułów (chyba że dany moduł został wprost wskazany jako opcjonalny).	

Lp.	Wymaganie ogólne	Spełnia (TAK/NIE)
4	Konsola administracyjna oraz dokumentacja techniczna muszą być dostępne co najmniej w języku polskim lub angielskim; dokumentacja powykonawcza zostanie dostarczona w języku polskim.	
5	Przetwarzanie danych (w tym treści wiadomości e-mail i danych osobowych) musi odbywać się zgodnie z RODO; Wykonawca zawrze z Zamawiającym umowę powierzenia przetwarzania danych osobowych wg wzoru dostarczonego przez Zamawiającego. Przetwarzanie danych musi co do zasady odbywać się na terenie Europejskiego Obszaru Gospodarczego (EOG); jedyny dopuszczalny wyjątek dotyczy funkcjonalności sprawdzania adresów URL, na zasadach określonych w punktach poniżej.	
6	Rozwiązanie musi zapewniać interoperacyjność z istniejącym środowiskiem teleinformatycznym Zamawiającego (poczta, usługa katalogowa). Wskazane w opisie nazwy systemów (np. Active Directory, Azure AD / Microsoft Entra ID, Microsoft 365, Microsoft Exchange, Microsoft Outlook, OWA, OneDrive, SharePoint, Google Workspace) służą wyłącznie opisaniu środowiska Zamawiającego oraz zapewnieniu interoperacyjności i nie stanowią preferencji wobec konkretnego producenta rozwiązania bezpieczeństwa.	
7	Rozwiązanie musi być wdrożone w modelu hybrydowym. Podstawowe moduły zabezpieczające (warstwa bramy pocztowej, w szczególności agent MTA, silnik polityk bezpieczeństwa, antyspam, antywirus, kwarantanna oraz lokalny magazyn danych pocztowych) muszą być wdrożone i eksploatowane w modelu lokalnym (on-premise), w infrastrukturze Zamawiającego. Zaawansowane funkcjonalności analizy zagrożeń (analiza załączników w środowisku sandbox oraz analiza i ochrona adresów URL) mogą być realizowane jako usługi chmurowe producenta, z zachowaniem wymagań dotyczących lokalizacji przetwarzania danych określonych w punktach poniżej.	
8	Podstawowe moduły zabezpieczające, stanowiące warstwę on-premise rozwiązania, muszą być możliwe do uruchomienia jako maszyny wirtualne w aktualnie eksploatowanym przez Zamawiającego środowisku wirtualizacyjnym VMware vSphere 8. Wymóg ten wynika z konieczności zapewnienia interoperacyjności z istniejącą infrastrukturą Zamawiającego i nie stanowi preferencji dla producenta platformy wirtualizacyjnej ani producenta rozwiązania bezpieczeństwa poczty. Wykonawca dostarczy obraz maszyny wirtualnej w formacie OVA/OVF albo inny pakiet instalacyjny, obraz, template lub równoważny mechanizm wdrożeniowy umożliwiający instalację i uruchomienie rozwiązania w środowisku VMware vSphere 8 bez konieczności nabywania przez Zamawiającego dodatkowej platformy wirtualizacyjnej. Za zgodność ze środowiskiem Zamawiającego uznaje się co najmniej możliwość importu, instalacji, uruchomienia, aktualizacji i wsparcia producenta dla rozwiązania działającego w środowisku VMware vSphere 8. Wykonawca dostarczy dokumentację instalacyjną i konfiguracyjną oraz wskaże wymagane zasoby maszyny wirtualnej.	

Lp.	Wymaganie ogólne	Spełnia (TAK/NIE)
9	Rozwiązanie musi umożliwiać dodawanie kolejnych wirtualnych instancji / agentów (skalowanie poziome) w celu zwiększenia wydajności, rozłożenia obciążenia oraz zapewnienia wysokiej dostępności, bez konieczności nabywania dodatkowych licencji. Licencjonowanie musi być oparte o liczbę chronionych użytkowników (4 500), niezależnie od liczby uruchomionych instancji / agentów wirtualnych oraz niezależnie od liczby obsługiwanych domen pocztowych. Również wsparcie techniczne i utrzymanie producenta nie mogą być uzależnione od liczby uruchomionych instancji / agentów wirtualnych, lecz wyłącznie od liczby chronionych użytkowników.	
10	Skanowanie i analiza załączników (w tym analiza dynamiczna / detonacja w środowisku typu sandbox), niezależnie od tego, czy realizowane lokalnie czy jako usługa chmurowa, musi odbywać się wyłącznie na terenie Europejskiego Obszaru Gospodarczego (EOG). Dane załączników (treść plików) nie mogą być przekazywane ani przetwarzane poza EOG.	
11	Funkcjonalność sprawdzania i analizy adresów URL (linków) może wykorzystywać przetwarzanie z transferem danych do państwa trzeciego (poza EOG) wyłącznie pod warunkiem, że producent rozwiązania posiada odpowiednie instrumenty zapewniające zgodność takiego transferu z RODO (np. decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony, standardowe klauzule umowne (SCC) lub udział w programie EU-US Data Privacy Framework). Wykonawca wskaże podstawę prawną oraz mechanizm transferu danych realizowanego w ramach tej funkcjonalności.	
12	Dostarczany obraz maszyny wirtualnej spełnia co najmniej minimalne wymagania zasobowe określone w Sekcji IV OPZ dla węzła zarządzającego (master) oraz węzła przetwarzającego (agent).	

Część B. Wymagania minimalne (obligatoryjne)

1. Wdrażanie i zarządzanie

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
1	Oferowane rozwiązanie musi być przedmiotem aktualnej, niezależnej oceny rynkowej przeprowadzonej przez renomowaną organizację analityczną w obszarze bezpieczeństwa poczty elektronicznej (np. Gartner, Forrester Wave, Frost Radar).	
2	Podstawowe moduły zabezpieczające (warstwa bramy pocztowej) muszą być możliwe do wdrożenia w modelu lokalnym (on-premise) w infrastrukturze Zamawiającego; zaawansowane funkcje analizy zagrożeń (analiza załączników w środowisku sandbox oraz analiza i ochrona adresów URL) mogą być świadczone jako usługi chmurowe producenta, zgodnie z wymaganiami dotyczącymi lokalizacji przetwarzania danych określonymi w Sekcji IV.	
3	Rozwiązanie musi udostępniać narzędzia lub interfejs programistyczny (API) umożliwiający integrację z rozwiązaniami bezpieczeństwa innych producentów w celu rozszerzenia funkcjonalności.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
4	Rozwiązanie musi umożliwiać szybką i bezproblemową konfigurację bez konieczności zmiany rekordów MX, a także — alternatywnie — wdrożenie w oparciu o rekordy MX.	
5	Wykonawca, w przypadku wykupienia dodatkowej usługi serwisowej wykraczającej poza wsparcie producenta, musi zapewnić wsparcie co najmniej w godzinach pracy Zamawiającego.	
6	Rozwiązanie musi udostępniać konfigurowalny portal zarządzania z kontrolą dostępu opartą na rolach (RBAC), dostosowaną do uprawnień i wymagań użytkownika.	
7	Rozwiązanie musi zapewniać zdefiniowaną, regularną częstotliwość aktualizacji i poprawek platformy bezpieczeństwa poczty elektronicznej (Wykonawca wskaże częstotliwość: miesięczna / kwartalna / roczna).	
8	Rozwiązanie musi obsługiwać synchronizację użytkowników i grup zarówno z lokalną usługą katalogową Active Directory (poprzez mechanizm push lub protokół LDAPs), jak i z usługą Azure AD / Microsoft Entra ID lub równoważną.	
9	Rozwiązanie musi umożliwiać integrację ze standardem SAML 2.0 w celu uwierzytelniania i bezpiecznego dostępu.	
10	Rozwiązanie musi zapewniać mechanizm jednokrotnego logowania (SSO) z usługą katalogową lub mechanizm synchronizacji haseł, umożliwiający użytkownikom korzystanie ze standardowych poświadczeń domenowych.	
11	Rozwiązanie musi umożliwiać ograniczenie dostępu do portalu administracyjnego na podstawie określonych adresów IP.	
12	Rozwiązanie musi umożliwiać przydzielenie dedykowanych, statycznych, publicznych adresów IP wyłącznie dla Zamawiającego (nieudostępnianych innym podmiotom) — zarówno dla ruchu wychodzącego, jak i przychodzącego.	
13	Rozwiązanie musi udostępniać interfejs administracyjny umożliwiający skuteczne śledzenie przepływu wiadomości e-mail (message tracking) oraz monitorowanie i analizę transakcji pocztowych.	
14	Wykonawca musi udostępnić na żądanie środowisko testowe UAT (User Acceptance Testing) umożliwiające przetestowanie i walidację rozwiązania.	
15	Rozwiązanie musi integrować się z lokalnym serwerem poczty elektronicznej Zamawiającego oraz pakietem biurowym eksploatowanym przez Zamawiającego (lub środowiskiem równoważnym), zapewniając łatwe wdrożenie i zarządzanie.	
16	Rozwiązanie musi udostępniać interfejs zarządzania politykami umożliwiający konfigurowanie złożonych, zagnieżdżonych reguł dla ruchu przychodzącego i wychodzącego.	
17	Rozwiązanie musi udostępniać interfejs zarządzania politykami z możliwością kwarantanny wiadomości na podstawie zdefiniowanych reguł, z możliwością przekierowania wiadomości do administratora/SOC i ich późniejszego zwolnienia do użytkowników.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
18	Rozwiązanie musi obsługiwać wymuszony protokół TLS w wersji co najmniej 1.2 dla ruchu przychodzącego i wychodzącego.	
19	Rozwiązanie musi szyfrować dane przechowywane (w spoczynku) — w tym przechowywane wiadomości, kwarantannę oraz dzienniki zdarzeń — a także dane przesyłane (w trakcie transmisji).	
20	Rozwiązanie musi integrować się z lokalnymi bramami pocztowymi poprzez przekazywanie wiadomości za pośrednictwem agenta MTA (relay).	
21	Rozwiązanie musi obsługiwać zarówno odbieranie poczty przychodzącej, jak i wysyłanie poczty wychodzącej, pełniąc rolę bramy / agenta MTA dla obu kierunków przepływu poczty.	
22	Rozwiązanie musi obsługiwać wiele domen pocztowych Zamawiającego — zarówno przy odbieraniu, jak i wysyłaniu poczty — bez dodatkowych opłat licencyjnych uzależnionych od liczby obsługiwanych domen.	
23	Rozwiązanie musi umożliwiać przechowywanie kopii wiadomości e-mail w pierwszym punkcie wejścia przez ograniczony czas, na potrzeby analizy i dochodzeń kryminalistycznych (zapewnienie wiarygodnego, dostępnego źródła danych do analizy).	

2. Ochrona przed przejęciem biznesowej poczty e-mail (BEC)

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
24	Rozwiązanie musi wykorzystywać technologię antyphishingową opartą na AI/ML do wykrywania wzorców komunikacji i anomalii w stylu konwersacji oraz analizę obrazu (computer vision) do badania podejrzanych adresów URL, zapewniając ukierunkowaną ochronę przed atakami BEC.	
25	Rozwiązanie musi dynamicznie analizować zawartość nagłówków oraz treści wiadomości w celu wykrywania ataków polegających na podszywaniu się pod domenę, podszywaniu się pod nazwę wyświetlaną oraz rejestracji domen łudząco podobnych (typosquatting).	
26	Rozwiązanie musi zawierać klasyfikator wykrywający oszustów (impostor), wykorzystujący złożoną ocenę spamu i uczenie maszynowe do rozpoznawania wzorców ruchu pocztowego organizacji oraz proaktywnej ochrony przed atakami BEC.	
27	Rozwiązanie musi zapewniać analizę łańcucha dostaw oraz łańcucha kontaktów opartą na AI/ML w celu identyfikacji i obrony przed atakami socjotechnicznymi, podszywaniem się oraz BEC.	

3. Phishing, ransomware i złośliwe oprogramowanie

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
28	Rozwiązanie musi zapewniać kompleksową ochronę przed atakami phishingowymi, w tym zaawansowaną ochronę przed phishingiem, wykrywanie oszustów oraz ochronę poczty wewnętrznej.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
29	Rozwiązanie musi proaktywnie analizować podejrzone adresy URL w środowisku sandbox z użyciem analizy dynamicznej/behawioralnej, aby zapobiegać rozprzestrzenianiu się złośliwego oprogramowania i innych zagrożeń.	
30	Rozwiązanie musi blokować złośliwe adresy URL, wykorzystywać przepisywanie adresów URL oraz udostępniać konfigurowalne strony blokady dla niebezpiecznych witryn (edukacja użytkowników).	
31	Rozwiązanie musi wykorzystywać technologie AI/ML w celu zwiększenia skuteczności wykrywania zagrożeń w poczcie elektronicznej.	
32	Rozwiązanie musi wykorzystywać AI/ML do analizy wzorców komunikacji w celu zapobiegania przychodzącemu phishingowi oraz wykrywania potencjalnie błędnie zaadresowanych wiadomości.	
33	Rozwiązanie musi umożliwiać tworzenie niestandardowych reguł antyphishingowych oraz analizę AI/ML do wykrywania ukierunkowanych ataków phishingowych o niskiej skali.	
34	Rozwiązanie musi zapewniać integrację API z platformami współpracy w celu filtrowania złośliwych treści lub podejrzanych interakcji.	
35	Rozwiązanie musi zapewniać ochronę przed atakami DoS oraz zbieraniem katalogów (directory harvesting) w celu zachowania dostępności usług poczty.	
36	Rozwiązanie musi zapewniać ochronę przed atakami wykradającymi poświadczenia (wiadomości phishingowe kierujące do fałszywych stron logowania).	
37	Rozwiązanie musi zapewniać ochronę przed spear-phishingiem, w szczególności przed opóźnionymi exploitami.	
38	Rozwiązanie musi być zdolne do przeprowadzania analizy z wykorzystaniem technik przeciwdziałających uchylaniu się od wykrycia (anti-evasion).	
39	Rozwiązanie musi obsługiwać przepisywanie adresów URL dla wiadomości przychodzących, zapewniając bezpieczne wykonanie za pośrednictwem platformy izolacji.	
40	Rozwiązanie musi przeprowadzać inspekcję adresów URL w czasie rzeczywistym w treści wiadomości, załącznikach (PDF, dokumenty pakietu biurowego itp.) oraz w serwisach udostępniania plików (np. OneDrive, SharePoint lub równoważnych).	
41	Rozwiązanie musi wykorzystywać analizę obrazu AI/ML do wykrywania i blokowania złośliwych adresów URL.	
42	Rozwiązanie musi blokować adresy URL na podstawie reputacji jeszcze przed dostarczeniem, z wykorzystaniem analizy predykcyjnej.	
43	Rozwiązanie musi obsługiwać ochronę adresów URL po dostarczeniu (np. analizę zawartości adresu URL w sandbox).	
44	Rozwiązanie musi stale i wstecznie analizować złośliwe adresy URL po dostarczeniu oraz umożliwiać administratorom usuwanie wiadomości, których dotyczy problem (monitorowanie zachowania adresu URL pod kątem opóźnionych ataków).	
45	Rozwiązanie musi umożliwiać weryfikację adresów URL w wiadomościach na podstawie czasu kliknięcia (time-of-click).	

Załącznik nr 2 do umowy

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
46	Rozwiązanie musi zapewniać izolowane środowiska kontenerowe (tylko do odczytu) do wykonywania podejrzanych adresów URL i linków w wiadomościach lub załącznikach.	
47	Rozwiązanie musi umożliwiać dekodowanie przepisanych adresów URL w celu identyfikacji oryginalnej witryny docelowej.	
48	Rozwiązanie musi utrzymywać dostarczanie wiadomości w trakcie analizy wszystkich adresów URL i linków zawartych w wiadomości.	
49	Rozwiązanie musi umożliwiać administratorom nadpisywanie blokad adresów URL i podejmowanie świadomych decyzji o zezwoleniu.	
50	Rozwiązanie musi umożliwiać izolację stron internetowych i wymuszać tryb tylko do odczytu, aby zapobiec nieautoryzowanemu przesyłaniu poświadczeń i danych użytkownika.	
51	Rozwiązanie musi bezpiecznie przechowywać dane wiadomości i załączników na platformie izolacji.	
52	Rozwiązanie musi realizować analizę typu sandbox (detonację) załączników w środowisku zlokalizowanym wyłącznie na terenie EOG — lokalnie w infrastrukturze Zamawiającego lub w chmurze prywatnej/publicznej w regionie EOG; dane załączników nie mogą być przekazywane poza EOG (zob. Sekcja IV).	

4. Raportowanie i korygowanie wiadomości e-mail

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
53	Rozwiązanie musi umożliwiać połączenie ze skrzynką nadużyć (abuse mailbox) i automatyzację usuwania wiadomości wysłanych do tej skrzynki.	
54	Rozwiązanie musi obsługiwać API umożliwiające integrację zdarzeń poczty z systemami XDR, SIEM oraz mSOAR.	
55	Rozwiązanie musi obsługiwać zautomatyzowane korygowanie dostarczonych zagrożeń.	
56	Rozwiązanie musi umożliwiać administratorom analizowanie i przenoszenie złośliwych lub niechcianych wiadomości do kwarantanny po dostarczeniu.	
57	Rozwiązanie musi wykrywać i usuwać złośliwe wiadomości przekazane wewnętrznie.	
58	Rozwiązanie musi zapewniać mechanizm ręcznego przeglądu wiadomości z możliwością śledzenia działań użytkownika.	
59	Rozwiązanie musi obsługiwać ręczne usuwanie wiadomości ze skrzynek z wykorzystaniem formatu pliku JSON.	
60	Rozwiązanie musi konsolidować alerty z wielu źródeł i korelować je w jedno zdarzenie.	
61	Rozwiązanie musi wykorzystywać informacje o zagrożeniach (threat intelligence) z różnych źródeł i automatycznie wzbogacać alerty.	
62	Rozwiązanie musi zapewniać automatyczną kwarantannę i powstrzymywanie zagrożeń lub proste działania ochronne dla szybkiej reakcji.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
63	Rozwiązanie musi automatyzować zarządzanie użytkownikami, wiadomościami, hostami, adresami IP i URL w systemach egzekwowania podczas ataku.	
64	Rozwiązanie musi udostępniać banery kontekstowe ostrzegające użytkowników oraz przycisk zgłaszania wiadomości nie wymagający instalacji.	
65	Rozwiązanie musi wyświetlać banery HTML w klientach poczty, automatycznie przełączając się na format zwykłego tekstu, gdy HTML nie jest obsługiwany, z obsługą wielu języków i możliwością edycji treści banera przez organizację.	
66	Rozwiązanie musi automatycznie analizować wiadomości zgłoszone przez użytkowników w celu weryfikacji ich złośliwego charakteru.	
67	Rozwiązanie musi integrować się z narzędziami mSOAR w celu automatyzacji procesu zgłaszania złośliwych wiadomości, w tym ich przeklasyfikowania i usuwania ze skrzynek.	
68	Rozwiązanie musi umożliwiać dodanie szyfrowania do wiadomości w celu zapobiegania nieautoryzowanemu dostępowi do treści.	
69	Rozwiązanie musi analizować treść wiadomości i umożliwiać blokowanie, przekierowanie lub szyfrowanie wiadomości na podstawie tej analizy.	
70	Rozwiązanie musi umożliwiać zabezpieczanie, śledzenie i ewentualną redakcję poufnych danych udostępnianych w wiadomościach partnerom i klientom.	
71	Rozwiązanie musi oferować wiele opcji obsługi zagrożeń, w tym usuwanie załączników, powiadamianie nadawców oraz kwarantannę całej wiadomości.	
72	Rozwiązanie musi udostępniać administratorom funkcję „Bezpieczny podgląd” do wyświetlania szczegółów wiadomości w kwarantannie i podejmowania decyzji o niezbędnych akcjach.	
73	Rozwiązanie musi umożliwiać użytkownikom końcowym zgłaszanie wyników fałszywie ujemnych i fałszywie dodatnich.	
74	Rozwiązanie musi automatycznie usuwać/wycofywać wszystkie wiadomości uznane za złośliwe po dostarczeniu.	
75	Rozwiązanie musi pozyskiwać wiadomości zgłaszane przez użytkowników z różnych źródeł, w tym ze skrzynki nadużyć, dodatku do klienta poczty oraz dynamicznych banerów HTML.	
76	Rozwiązanie musi automatyzować reakcje przy użyciu predefiniowanych zestawów reguł lub playbooków dla różnych zadań, w tym badania alertów, oceny wpływu i działań naprawczych.	
77	Rozwiązanie musi automatyzować reakcje na wiadomości przekazane oraz podobne wiadomości dostarczone użytkownikom, w szczególności gdy zostaną zidentyfikowane jako złośliwe.	
78	Rozwiązanie musi umożliwiać przypisywanie poziomów ważności lub ocen wykrytym zagrożeniom, umożliwiając skuteczną priorytetyzację i alokację zasobów.	
79	Rozwiązanie musi udostępniać kompleksowy portal umożliwiający dostęp do informacji i metadanych o zdarzeniach/incydentach na potrzeby analizy zagrożeń.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
80	Rozwiązanie musi umożliwiać zespołom bezpieczeństwa i osobom reagującym na incydenty automatyzację identyfikacji, korygowania i udostępniania zagrożeń phishingowych.	
81	Rozwiązanie musi przekazywać użytkownikom informacje zwrotne w zależności od typu zgłaszanej wiadomości, umożliwiając zamykanie zgłoszeń i oferując terminowe aktualizacje lub rozwiązania.	
82	Rozwiązanie musi zapewniać osobom reagującym na incydenty analizę w czasie rzeczywistym oraz wgląd w ataki pocztowe wymierzone w organizację.	

5. Pulpity nawigacyjne oraz raporty o zagrożeniach i użytkownikach

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
83	Rozwiązanie musi zapewniać widoczność zagrożeń bezpieczeństwa w organizacji, w tym: najczęściej atakowane konta e-mail, sposób ataku na te konta, użytkowników o zachowaniach wysokiego ryzyka oraz sposób uzyskiwania przez nich dostępu do danych.	
84	Rozwiązanie musi dostarczać raport podsumowujący dla kadry zarządzającej, obejmujący m.in.: filtry czasowe, liczbę wiadomości przychodzących/wychodzących, spam, wiadomości masowe, phishing, wiadomości złośliwe (AV, antymalware, sandbox), najczęstsze złośliwe adresy URL i złe domeny oraz ataki ukierunkowane z wybranego obszaru geograficznego.	
85	Rozwiązanie musi umożliwiać segmentację/filtrowanie danych raportowych wg kryteriów, np. kraju, hierarchii organizacyjnej, jednostek biznesowych, działów, opisu stanowiska oraz typu wektora ataku (spam, malware, phishing, złośliwe adresy URL, złe domeny).	
86	Rozwiązanie musi zapewniać szczegółową, bogatą w kontekst i umożliwiającą podejmowanie działań analizę zagrożeń, w tym wskaźniki naruszenia bezpieczeństwa (IOC) oraz informacje o odbiorcach.	
87	Producent powinien dysponować centrum analizy zagrożeń lub łączyć się z nim w celu zapewnienia branżowego testu porównawczego oraz automatycznej aktualizacji i wzbogacania alertów.	
88	Rozwiązanie musi zapewniać szczegółowe raporty obejmujące użycie systemu (globalne podsumowanie wiadomości, spam, wirusy, działania reguł) z możliwością wysyłki e-mail (HTML), druku lub pobrania w formacie CSV.	
89	Rozwiązanie musi umożliwiać administratorom wyświetlanie raportów ze szczegółowymi statystykami przetworzonych i odrzuconych wiadomości, transakcji SMTP oraz przepływów komunikacji.	
90	Rozwiązanie musi umożliwiać porównanie liczby i dotkliwości ataków z innymi organizacjami z branży lub grupami porównawczymi.	
91	Rozwiązanie musi dostarczać informacje o podmiotach (aktorach) atakujących organizację.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
92	Rozwiązanie musi rozpoznawać, czy wiadomości stanowią część kampanii ukierunkowanej na organizację.	
93	Rozwiązanie musi udostępniać administratorom zaawansowane pulpity zagrożeń zawierające trendy i analizy malware/spamu, analizę sandbox, kliknięcia adresów URL oraz próby phishingu.	
94	Rozwiązanie musi zawierać raporty o zamiarach atakujących (np. malware, kradzież poświadczeń, podszywanie się) oraz próbach ransomware (np. broker dostępu pocztowego).	
95	Rozwiązanie musi zapewniać szczegółowe raportowanie liczby i typów wiadomości zgłaszanych przez użytkowników oraz rozumienie trendów ataków wpływających na organizację.	
96	Rozwiązanie musi dostarczać szczegółowe informacje oparte na ryzyku oraz rekomendować kontrolę zabezpieczeń na podstawie tych informacji.	
97	Rozwiązanie musi zapewniać eksport danych przez API w celu integracji z SOC.	
98	Rozwiązanie musi umożliwiać administratorom szybkie generowanie raportów w czasie rzeczywistym w interfejsie zarządzania.	
99	Rozwiązanie musi umożliwiać monitorowanie i porównywanie z innymi firmami z branży w ujęciu pionowym (benchmark).	
100	Rozwiązanie musi obsługiwać pełną inspekcję wiadomości przychodzących i wychodzących.	
101	Rozwiązanie musi zapewniać prostotę oceny oraz dodatkowy wgląd w ruch wewnętrzny i inne kanały komunikacji, a także w aktywność wychodzącą użytkowników w celu wykrywania podejrzanych zachowań.	
102	Rozwiązanie musi zapewniać praktyczny pulpit zagrożeń umożliwiający tworzenie usprawnionych przepływów pracy do szybkiego reagowania na zagrożenia związane z malware/wirusami przesyłanymi pocztą.	

6. Higiena i konfiguracja poczty przychodzącej

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
103	Rozwiązanie musi obsługiwać dokładne wykrywanie i blokowanie złośliwych wiadomości z wykorzystaniem automatycznej analizy malware, w tym: blokowanie wiadomości od znanych nieprawidłowych nadawców, skanowanie załączników programem antywirusowym, blokowanie wiadomości ze znanymi złośliwymi adresami URL oraz analizę treści w celu identyfikacji spamu.	
104	Rozwiązanie musi posiadać zaawansowane możliwości ochrony, w tym: przepisywanie adresów URL, skanowanie antywirusowe, integrację z sandbox, kwarantannę spamu z podsumowaniami dla użytkowników końcowych, obsługę niechcianych wiadomości masowych (tzw. graymail), ochronę BEC oraz wycofanie po dostarczeniu.	
105	Rozwiązanie musi charakteryzować się wysoką skutecznością w wykrywaniu spamu.	
106	Rozwiązanie musi zapewniać wysoką dostępność usług, odpowiadającą potrzebom biznesowym Zamawiającego.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
107	Rozwiązanie musi zapewniać pełną ochronę przed znanymi zagrożeniami ze strony złośliwego oprogramowania.	
108	Rozwiązanie musi utrzymywać niski wskaźnik wyników fałszywie dodatnich przy jednoczesnym skutecznym identyfikowaniu i blokowaniu złośliwej zawartości.	
109	Rozwiązanie musi zapewniać niskie opóźnienia w dostarczaniu poczty.	
110	Rozwiązanie musi skutecznie i terminowo skanować oraz zwalniać załączniki.	
111	Rozwiązanie musi umożliwiać terminową identyfikację i śledzenie wiadomości po ich wysłaniu.	
112	Rozwiązanie musi obsługiwać zarządzanie klasyfikacją wiadomości, w tym oddzielne klasyfikatory dla spamu, podszywania się, wiadomości masowych, phishingu, treści dla dorosłych i malware, z możliwością ustawiania progów punktacji dla każdej kategorii.	
113	Rozwiązanie musi obsługiwać skanowanie i stosowanie reguł dla plików zaszyfrowanych lub chronionych hasłem oraz wielokrotnie skompresowanych.	
114	Rozwiązanie musi obsługiwać precyzyjne dostrajanie poziomu wykrywania spamu.	
115	Rozwiązanie musi obsługiwać wykrywanie nowych kampanii spamowych.	
116	Rozwiązanie musi automatycznie usuwać podejrzane wiadomości ze skrzynek odbiorczych użytkowników.	
117	Rozwiązanie musi zapewniać szczegółowe mechanizmy kontroli administracyjnej z dostępem opartym na rolach do każdego modułu i folderu kwarantanny.	
118	Rozwiązanie musi zezwalać użytkownikowi końcowemu na dostęp do niezłośliwych wiadomości w kwarantannie, jednocześnie uniemożliwiając dostęp do wiadomości złośliwych.	
119	Rozwiązanie musi spełniać złożone wymagania dotyczące routingu poczty, w tym routingu opartego na grupach użytkowników.	
120	Rozwiązanie musi korzystać z zaawansowanych technik ochrony przed kradzieżą poświadczeń oraz analizy obrazu w celu wykrywania i blokowania ataków phishingowych podszywających się pod strony logowania.	
121	Rozwiązanie musi wykorzystywać uczenie maszynowe do ciągłego monitorowania i dostosowywania się do wzorców komunikacji e-mail w organizacji.	
122	Rozwiązanie musi generować logi w widoku zbliżonym do czasu rzeczywistego oraz oferować wydajne wyszukiwanie danych dziennika z zaawansowanymi filtrami.	
123	Rozwiązanie musi obsługiwać integrację z zewnętrznymi magazynami danych i bazami danych.	
124	Rozwiązanie musi zapewniać skuteczne wykrywanie spamu w wielu językach, w tym m.in. chińskim (uproszczonym i tradycyjnym), angielskim, japońskim, koreańskim, tajskim i wietnamskim.	
125	Rozwiązanie musi umożliwiać administratorom przypisywanie różnych zestawów reguł na podstawie określonych adresów e-mail.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
126	Rozwiązanie musi oferować weryfikację odbiorcy w usłudze katalogowej oraz innych źródłach list e-mail, aby zapobiegać spoofingowi i usprawniać dostarczanie wiadomości.	
127	Rozwiązanie musi obsługiwać szeroki zakres zachowań i akcji routingu dla różnych scenariuszy obsługi poczty.	
128	Rozwiązanie musi umożliwiać zarządzanie stopkami w wiadomościach przychodzących i wychodzących, w tym: wstawianie stopek prawnych i zgodności (np. klauzul poufności), obsługę wielu języków, stosowanie filtrów na podstawie atrybutów wiadomości lub Active Directory, wstawianie treści dynamicznej (np. daty), warunkowe stosowanie w określonych przeskokach routingu, selektywne stosowanie na podstawie polityki/attributu, pomijanie dla wiadomości szyfrowanych S/MIME lub podpisanych cyfrowo oraz stosowanie podpisów i zastrzeżeń na podstawie grup użytkowników AD.	
129	Rozwiązanie musi umożliwiać użytkownikom końcowym otrzymywanie niestandardowych powiadomień e-mail na podstawie nazwy domeny.	
130	Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe dla użytkowników końcowych, administratorów platformy i administratorów systemu.	
131	Rozwiązanie musi zapewniać internetową konsolę zarządzania i konfiguracji centralizującą konfigurację, rejestrowanie, kwarantannę i raportowanie, kompatybilną z nowoczesnymi przeglądarkami.	
132	Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach do konsoli zarządzania, z możliwością przypisania nazwanym kontom administratorów określonych uprawnień; konsola musi obsługiwać usługę katalogową i uwierzytelnianie wieloskładnikowe.	
133	Rozwiązanie musi zapewniać administratorom możliwość zarządzania kolejką poczty e-mail.	
134	Rozwiązanie musi umożliwiać delegowanie administracji do podorganizacji w oparciu o logiczne grupowania użytkowników (jednostki biznesowe, regiony, role, funkcje, hierarchia), z dziedziczeniem zasad z organizacji głównej oraz możliwością ich nadpisywania.	
135	Rozwiązanie musi obsługiwać powiadamianie zespołu bezpieczeństwa o wszystkich zasadach, folderach kwarantanny i progach kolejki.	
136	Rozwiązanie musi umożliwiać ograniczenie rozmiaru wysyłanych/odbieranych wiadomości lub liczby adresatów.	
137	Rozwiązanie musi umożliwiać ograniczenie sondowania SMTP oraz walidację informacji na kopercie przed przyjęciem wiadomości do dostarczenia.	
138	Rozwiązanie musi zapewniać narzędzia do diagnozowania problemów z routingiem aplikacji i wiadomości, z możliwością śledzenia wiadomości (message trace) wspierającą pomoc techniczną.	
139	Rozwiązanie musi umożliwiać dołączanie słów kluczowych do tematu, nagłówka i treści wiadomości na podstawie zestawu reguł.	
140	Rozwiązanie musi obsługiwać tworzenie list bezpiecznych/zablokowanych na podstawie użytkowników lub grup użytkowników.	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
141	Rozwiązanie musi obsługiwać importowanie wielu użytkowników/grup do list bezpiecznych/zablokowanych z plików CSV/tekstowych.	
142	Rozwiązanie musi obsługiwać i filtrować biuletyny informacyjne oraz masowy spam.	
143	Rozwiązanie musi wykrywać ataki spamowe oparte na tekście, obrazach, multimediami i załącznikach.	
144	Rozwiązanie musi obsługiwać ukierunkowane blokowanie wiadomości spamowych.	
145	Rozwiązanie musi wykrywać kampanie spamowe i dodawać ich źródło do czarnej listy, natychmiast blokując połączenia z danego serwera pocztowego.	
146	Rozwiązanie musi zapewniać ochronę przed nękaniami pocztą i ograniczać ryzyko związane z wiadomościami od nieznanymi nadawców, szczególnie dla kadry kierowniczej i VIP.	
147	Rozwiązanie musi oferować możliwości analizy fałszerstw (spoofing) podszywających się pod domeny biznesowe.	
148	Rozwiązanie musi obsługiwać filtrowanie połączeń w oparciu o reputację (domeny lub adresy IP).	
149	Rozwiązanie musi integrować się z zewnętrznymi silnikami antywirusowymi i antymalware w celu filtrowania wiadomości.	
150	Rozwiązanie musi umożliwiać blokowanie określonych typów plików na podstawie rozszerzeń (np. .exe, .dll, .doc/.docx, .xls/.xlsx, .ppt/.pptx, .jpg, .png, .pdf, .swf, .mp3/.mp4, .java, .vbs).	
151	Rozwiązanie musi umożliwiać blokowanie archiwów załączników (np. .zip, .tgz, .7z, .cab, .lzh, .rar, .tnef).	

7. Obsługa DMARC w systemie ochrony poczty

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
152	Weryfikacja i egzekwowanie DMARC (ruch przychodzący). System musi zapewniać weryfikację wiadomości przychodzących w oparciu o mechanizmy SPF, DKIM i DMARC, sprawdzanie zgodności (alignment) domen pomiędzy nagłówkami SPF/DKIM a domeną nadawcy, identyfikację statusu DMARC (pass/fail/none) oraz wykorzystanie wyniku DMARC jako warunku w politykach bezpieczeństwa.	
153	Polityki bezpieczeństwa oparte o DMARC. System musi umożliwiać definiowanie granularnych polityk przetwarzania wiadomości w oparciu o wynik DMARC, w tym: kwarantannę wiadomości niespełniających DMARC, odrzucenie wiadomości (reject), oznaczanie/tagowanie (np. modyfikacja tematu lub nagłówków) oraz przepuszczanie wiadomości (allow) w uzasadnionych przypadkach; musi umożliwiać łączenie wyniku DMARC z dodatkowymi warunkami (grupy użytkowników, VIP, inne sygnały) oraz definiowanie wyjątków (zaufani nadawcy, scenariusze forwardingu).	
154	Tryb monitorowania (non-blocking). System musi umożliwiać wdrożenie polityk DMARC w trybie monitorowania (bez blokowania ruchu) oraz stopniowe zaostrowanie polityk (od monitorowania, przez kwarantannę, po odrzucanie).	

Lp.	Wymaganie minimalne	Spełnia (TAK/NIE)
155	Wsparcie dla mechanizmów uwierzytelniania (DMARC readiness). System musi wspierać konfigurację i obsługę podpisywania DKIM dla wiadomości wychodzących, w tym obsługę odrębnych kluczy i selektorów DKIM dla różnych domen nadawczych (obsługa wielu domen), integrację z istniejącą konfiguracją SPF po stronie Zamawiającego oraz obsługę wielu domen nadawczych.	
156	System musi obsługiwać zachowanie wyników uwierzytelniania wiadomości (SPF, DKIM, DMARC) przy przekazywaniu poczty przez serwery pośredniczące, na przykład przekierowania i listy dystrybucyjne (standard ARC), tak aby prawidłowo uwierzytelnione wiadomości nie były błędnie odrzucane po przejściu przez takie systemy.	
157	Widoczność i logowanie. System musi zapewniać widoczność wyników SPF, DKIM i DMARC dla przetwarzanych wiadomości, dostęp do logów umożliwiających analizę decyzji podjętych na podstawie DMARC, wyszukiwanie i filtrowanie wiadomości na podstawie statusu DMARC oraz wykorzystanie danych DMARC w raportach operacyjnych.	
158	Integracja z silnikiem polityk bezpieczeństwa. System musi umożliwiać wykorzystanie wyników DMARC jako jednego z wielu sygnałów w silniku decyzyjnym oraz wspierać centralne zarządzanie politykami bezpieczeństwa dla poczty przychodzącej.	

Część C. Oświadczenia w zakresie cyberbezpieczeństwa (KSC)

Wykonawca składa poniższe oświadczenie odnoszące się do całości oferowanego świadczenia (produkty ICT, usługi ICT i procesy ICT — zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi oraz rozwiązania towarzyszące).

Lp.	Oświadczenie	Potwierdzenie (TAK/NIE)
1	Oferowane świadczenie nie obejmuje produktów ICT, usług ICT ani procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa (stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa), ani produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka (art. 67b ust. 15 tej ustawy), ani usług ICT lub procesów ICT określonych w tej decyzji.	

Niespełnienie powyższego skutkuje odrzuceniem oferty odpowiednio na podstawie art. 226 ust. 1 pkt 17 albo pkt 19 ustawy Pzp.

Oświadczam, że informacje zawarte w powyższej matrycy są zgodne z prawdą, a oferowane rozwiązanie spełnia wszystkie wymagania minimalne oznaczone wyrazem TAK.

.....
podpis osoby upoważnionej do reprezentowania Wykonawcy