

Dostawa oraz wdrożenie oprogramowania przeznaczonego do podniesienia bezpieczeństwa systemu pocztowego Statystyki publicznej.

Przedmiotem zamówienia jest dostawa oprogramowania, w tym maszyn wirtualnych typu VA (*virtual appliance*) lub *appliance* sprzętowych wraz z licencjami i trzyletnim wsparciem producenta przeznaczonego do podniesienia bezpieczeństwa systemu pocztowego statystyki publicznej oraz wykonanie wdrożenia dostarczonych komponentów w infrastrukturze Zamawiającego w jego siedzibie w Warszawie przy al. Niepodległości 208.

W szczególności przedmiot zamówienia obejmuje następujące zadania do realizacji przez Wykonawcę:

- Zadanie 1:** Opracowanie Projektu technicznego
- Zadanie 2:** Dostawa oraz wdrożenie oprogramowania, w tym urządzeń wirtualnych typu *Virtual Appliance* lub *appliance* sprzętowego do zabezpieczenia transmisji wejściowych i wyjściowych danych pocztowych oraz zewnętrznych serwerów systemu pocztowego statystyki publicznej wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSZ (Systemem ochrony serwerów zewnętrznych).
- Zadanie 3:** Dostawa oraz wdrożenie oprogramowania do zabezpieczenia wewnętrznych serwerów pocztowych wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSW (Systemem ochrony serwerów wewnętrznych).
- Zadanie 4:** Wykonanie dokumentacji powykonawczej i przeprowadzenie warsztatów.

1. Wspólne uwarunkowania dla zadań oraz opis środowiska Zamawiającego

Prace wdrożeniowe i konfiguracyjne będą realizowane w Podstawowym Centrum Przetwarzania Danych mieszczącym się w siedzibie Zamawiającego w Warszawie.

Z uwagi na fakt, iż prace wdrożeniowe i rekonfiguracyjne będą prowadzone na działającym środowisku sprzętowo-systemowo-aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska, minimalizacja przestojów, szczegółowe zaplanowanie wszelkich prac oraz przygotowanie scenariuszy awaryjnych.

- 1.1. Zamawiający posiada domenę produkcyjną AD DS. (MS Active Directory) Windows Serwer 2019 o funkcjonalności lasu i domeny na poziomie Windows Server 2012R2.
- 1.2. Poczta korporacyjna statystyki publicznej działa w oparciu o MS Exchange Server 2019 RU14. System pocztowy jest scentralizowany – wszystkie serwery pocztowe znajdują się w Centrum Przetwarzania Danych w siedzibie Zamawiającego.
- 1.3. System poczty elektronicznej składa się z 6 serwerów:
 - 1.3.1. Czterech serwerów MS Exchange Mailbox (Multirole) Role, spiętych w klaster wysokiej dostępności DAG (*Database Availability Group*).
 - 1.3.2. Dwóch serwerów MS Exchange Edge Transport Server Role.
- 1.4. Na serwerach pocztowych zainstalowany jest system operacyjny MS Windows Server 2019.
- 1.5. Zamawiający dysponuje środowiskiem do wirtualizacji serwerów zbudowanym w oparciu o oprogramowanie VMware vSphere 8.
- 1.6. Do obsługi baz technicznych Zamawiający wykorzystuje oprogramowanie MS SQL 2019 Enterprise Edition.
- 1.7. Obecnie do ochrony zewnętrznego ruchu pocztowego Zamawiający wykorzystuje oprogramowanie FortiNet FortiMail Virtual Appliance 7.6 (FortiMail VM02).
- 1.8. Obecnie do ochrony wewnętrznych serwerów pocztowych Zamawiający wykorzystuje oprogramowanie ESET Mail Security for Microsoft Exchange 11.
- 1.9. Zamawiający dysponuje *sandbox'em on-premise*: Broadcom Symantec S500-A1.

2. Opis infrastruktury sprzętowo-systemowej posiadanej przez Zamawiającego i dedykowanej dla wdrożenia
 - 2.1. Zamawiający udostępni do dyspozycji Wykonawcy możliwość tworzenia niezbędnej liczby maszyn wirtualnych w środowisku VMware vSphere 8 wraz z licencjami serwerowymi MS Windows 2019, będącymi w posiadaniu Zamawiającego.
 - 2.2. Do utworzenia niezbędnych baz technicznych Zamawiający udostępni klaster MS SQL Server 2019 Enterprise posiadany przez Zamawiającego.
 - 2.3. W przypadku zaoferowania systemu, który nie będzie korzystał z udostępnionych przez Zamawiającego zasobów (pkt. 2.1, 2.2) i licencji, Wykonawca dostarczy wszystkie niezbędne elementy sprzętowe, systemowe i aplikacyjne.
3. Wymagania dotyczące bezpieczeństwa dostarczonego oprogramowania
 - 3.1. Dostarczone oprogramowanie nie może być zabronione do stosowania przez administrację któregokolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).
 - 3.2. Oferowany system musi być w całości posadowiony w siedzibie Zamawiającego. Zamawiający **nie dopuszcza** przekierowania ruchu SMTP z/do Zamawiającego na zewnętrzne serwery/usługi. Zamawiający dopuszcza posługiwanie się on-line przez system serwisami reputacyjnymi producenta rozwiązania.
4. **Zadanie 1:** Opracowanie Projektu Technicznego.

Wykonawca:

- 4.1. Przeprowadzi szczegółową analizę obecnie funkcjonującej infrastruktury i konfiguracji systemu pocztowego Zamawiającego.
- 4.2. Przygotuje i przekaze Zamawiającemu wraz z prawami autorskimi Projekt techniczny wdrożenia uzgodnionej koncepcji uwzględniający dobre praktyki rekomendacje eksploatacyjne publikowane przez producenta oprogramowania.
 - 4.2.1. Koncepcję wdrożenia oraz schematy połączeń dostarczanych komponentów.
 - 4.2.2. Wykaz dostarczanych urządzeń i licencji oprogramowania.
 - 4.2.3. Konfigurację i plan podłączenia systemu pocztowego do infrastruktury sieci LAN.
 - 4.2.4. Problematykę bezpieczeństwa informacji i zarządzania systemem pocztowym, w tym w szczególności z uwagi na konieczność oceny czy zachodzi powierzenie przetwarzania danych osobowych, projekt musi zawierać informację czy (a jeżeli tak to jakie dane osobowe i informacje) będą udostępniane poza infrastrukturę Zamawiającego celem prawidłowej realizacji umowy
 - 4.2.5. Opis backupowania i odtwarzania systemu pocztowego.
 - 4.2.6. Harmonogram realizacji przedmiotu zamówienia uwzględniający wszystkie aspekty techniczne, organizacyjne oraz terminowe przedmiotowej umowy.
 - 4.2.7. Projekt Testów Akceptacyjnych wdrożenia Systemu,.
 - 4.2.8. Projekt techniczny wdrożenia uzgodnionej koncepcji powinien uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta oprogramowania.

Procedura odbiorcza Zadania 1.

- 4.3. Projekt Techniczny „Dostawa oraz wdrożenie oprogramowania przeznaczonego do podniesienia bezpieczeństwa systemu pocztowego Statystyki publicznej” będzie podlegał procedurze odbioru, na następujących warunkach:

- 4.3.1. Wykonawca przekaze Zamawiającemu drogą elektroniczną do akceptacji Projekt Techniczny w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy.
 - 4.3.2. Zamawiający w terminie nie dłuższym niż 3 dni roboczych od dnia dostarczenia Projektu Technicznego, poinformuje Wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian.
 - 4.3.3. Wszystkie uwagi do Projektu Technicznego zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 3 dni roboczych d dnia ich otrzymania.
 - 4.3.4. Zamawiający w terminie 3 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionego Projektu Technicznego, poinformuje wykonawcę o jego akceptacji lub konieczności wprowadzenia zmian.
 - 4.3.5. Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w projekcie technicznym.
 - 4.3.6. W przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia Projektu Technicznego nie później niż po 5 dniach roboczych, po tym terminie Zamawiający ma prawo do odstąpienia od Umowy i zlecenia wykonawstwa zastępczego firmie trzeciej.
 - 4.3.7. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji Projektu Technicznego, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie.
 - 4.3.8. Zatwierdzony Projekt Techniczny zostanie przekazany Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru Zadania I na pendrive w wersji edytowalnej i PDF.
 - 4.4. Potwierdzeniem odbioru Projektu Technicznego będzie Protokół odbioru Zadania 1, podpisany z wynikiem pozytywnym.
5. **Zadanie 2:** Dostawa oraz wdrożenie oprogramowania, w tym *appliance* wirtualnych lub sprzętowych do zabezpieczenia transmisji wejściowych i wyjściowych danych pocztowych oraz zewnętrznych serwerów systemu pocztowego statystyki publicznej wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSZ (Systemem ochrony serwerów zewnętrznych)

Przedmiotem zadania jest dostawa oraz wdrożenie oprogramowania oraz urządzeń wirtualnych lub sprzętowych wraz z licencjami oraz trzyletnim wsparciem producenta pozwalającym na pobieranie aktualnych plików sygnatur, baz danych opisujących ataki, baz kategorii URL, instalację nowych wersji oprogramowania i korzystanie z pomocy technicznej producenta rozwiązania, dla 6500 użytkowników lub 7000 skrzynek pocztowych. Przy szacowanym obciążeniu 16000-18000 przesyłek przychodzących z Internetu i ok. 12000 przesyłek wychodzących dziennie do Internetu, przy maksymalnym obciążeniu 6000 przesyłek na godz.

Wymagania odnośnie licencji

- 5.1. Licencje mogą być dostarczone w pakiecie zawierającym różne funkcjonalności lub jako samodzielne produkty, ale muszą pochodzić od tego samego producenta. Zamawiający wymaga trzyletniego wsparcia producenta na zamawiane oprogramowanie. W przypadku wykorzystania maszyn wirtualnych na platformie VMware licencje muszą pozwalać na swobodne przenoszenie pomiędzy hostami VMware. Dostarczone licencje muszą umożliwiać wdrożenie co najmniej dwóch VA (*virtual appliance*) lub *appliance* sprzętowych lub większej liczby *appliance*, jeśli dostarczone rozwiązanie tego wymaga, w celu zapewnienia obsługi poczty nawet w wypadku awarii jednego z elementów.
- 5.2. Licencje muszą być dostarczone na produkt w najnowszej wersji i posiadający bieżące wsparcie producenta. Produkt (oprogramowanie) nie może znajdować się na liście „end of life” producenta, w momencie zaoferowania Zamawiającemu.

- 5.3. Zamawiający wymaga aby terminem rozpoczęcia biegu dostarczonych licencji rozpoczynał się w dniu 1 stycznia 2025 r. Jeżeli na czas wdrożenia i konfiguracji systemu wymagane jest objęcie licencją systemu SOSZ, Zamawiający wymaga dostarczenia dodatkowych licencji przejściowych (np. testowych).

Podstawowe wymagania funkcjonalne

- 5.4. Dostarczone rozwiązanie musi obsługiwać 6500 użytkowników lub 7000 skrzynek pocztowych Zamawiającego.
- 5.5. System SOSZ musi umożliwić ochronę ruchu pocztowego na poziomie 16000-18000 przesyłek przychodzących z Internetu i ok. 12000 przesyłek wychodzących dziennie do Internetu przy maksymalnym obciążeniu 6000 przesyłek na godz.
- 5.6. System SOSZ musi pracować w trybie bramki pocztowej SMTP w konfiguracji proxy aplikacyjnego (*mail gateway*).
- 5.7. Rozwiązanie ma działać w warstwie sieciowej i musi obsługiwać co najmniej protokół SMTP, przy czym musi być możliwe określenie portów na jakich działa protokół.
- 5.8. System SOSZ musi zapewnić zintegrowaną ochronę antyspamową, antywirusową oraz filtrowanie treści.
- 5.9. System SOSZ musi posiadać wbudowane wydajne mechanizmy ograniczania skutków ataków typu DoS (*Denial of Service*) i DDoS (*Distributed Denial of Service*) z wykorzystaniem poczty elektronicznej.
- 5.10. System SOSZ zbudowany w oparciu o maszyny wirtualne typu VA musi być kompatybilny z VMware vSphere 8 i nowszym.
- 5.11. System SOSZ musi być zbudowany w oparciu o elementy zapewniające wysoką dostępność, umożliwiające obsługę poczty nawet w wypadku awarii jednego z elementów systemu.
- 5.12. System SOSZ musi umożliwiać centralne zarządzanie wieloma maszynami wirtualnymi typu VA lub *appliance* sprzętowymi bez konieczności zakupu dodatkowych licencji lub oprogramowania.
- 5.13. Zarządzanie musi odbywać się poprzez konsolę zdalną. W przypadku gdy konsolą jest standardowa przeglądarka WWW połączenie musi być szyfrowane (https), korzystając z technologii TLS, w tym TLS1.3.
- 5.14. Interfejs zarządzający musi umożliwiać wizualizację przebiegu sesji protokołu SMTP i przejścia wiadomości przez poszczególne filtry ochronne.
- 5.15. System SOSZ musi posiadać wbudowane raportowanie, bez konieczności stosowania dodatkowego oprogramowania i zewnętrznych serwerów.
- 5.16. System musi umożliwiać weryfikację adresów email z serwerów LDAP w tym AD DS.
- 5.17. System SOSZ musi pozwalać na autentykację odbiorcy poczty i stworzenie polityki skanowania poczty uzależnionej od grup użytkowników lub poszczególnych użytkowników pochodzących z systemu poczty korporacyjnej statystyki publicznej.
- 5.18. Oprogramowanie musi pozwalać na stworzenie polityki skanowania zależnie od nazwy lub adresu IP domeny pocztowej, adresu źródłowego/docelowego użytkownika lub grupy użytkowników.
- 5.19. Musi być możliwe tworzenie osobnych polityk dla wiadomości wychodzących i dla przychodzących.
- 5.20. Musi być możliwe definiowanie równocześnie wielu polityk, których zastosowanie zależy od kolejności na liście polityk i w/w kryteriów.
- 5.21. Konfigurowanie polityk musi umożliwiać definiowanie kilku jednoczesnych reakcji na wykryte zdarzenie w tym na:
- 5.21.1. Zablokowanie wiadomości.
 - 5.21.2. Zablokowanie wiadomości i wystanie powiadomienia o tym zdarzeniu pod wskazany adres email.

- 5.21.3. Zablokowanie wiadomości i skierowanie jej do kwarantanny.
- 5.21.4. Przesłanie poczty do odbiorcy wraz z modyfikacją tytułu i nagłówka wiadomości.
- 5.21.5. Serwer nadawcy musi być powiadomiony o zablokowaniu wiadomości, niezależnie od przyczyny zablokowania, poprzez wygenerowanie odpowiedniego komunikatu SMTP w ramach jednej sesji SMTP.
- 5.22. System SOSZ musi usuwać z nagłówków wysyłanych wiadomości pocztowych informacje dotyczące wewnętrznej infrastruktury Zamawiającego.
- 5.23. Rozwiązanie, w ramach zdefiniowanych polityk, musi umożliwiać ograniczanie:
 - 5.23.1. Maksymalnej wielkości przesyłki pocztowej.
 - 5.23.2. Maksymalnej liczby załączników.
- 5.24. System SOSZ musi umożliwiać konfigurowanie polityk w zależności od nazwy, typu oraz rozszerzenia załącznika.
- 5.25. System SOSZ musi umożliwiać filtrowanie poczty na podstawie zawartości przesyłek (treści, załączników, atrybutów) w oparciu o słowa kluczowe, reguły, szablony, wbudowane i tworzone przez administratora słowniki.
- 5.26. System SOSZ musi umożliwiać szyfrowanie przesyłu poczty elektronicznej korzystając z technologii TLS, w tym TLS1.3.
- 5.27. System SOSZ musi umożliwiać podpisywanie wychodzących przesyłek kluczem DKIM.
 - 5.27.1. Moduł musi obsługiwać klucze DKIM o długości przynajmniej 2048 bity.
 - 5.27.2. Mechanizm wyliczania i umieszczania sygnatury w wiadomościach wysyłanych przez bramkę musi umożliwiać zarządzanie zarówno kluczami kryptograficznymi jak i regułami ich użycia. Moduł musi wspierać minimum następujące funkcje podpisywania wiadomości kluczem DKIM:
 - 5.27.2.1. Algorytmy podpisywania RSA-SHA-1 lub RSA-SHA-256,
 - 5.27.2.2. Możliwość podpisywania następujących nagłówków wiadomości: From, Reply-To, Subject, Date, To, Cc.
 - 5.27.2.3. Możliwość podpisywania własnych nagłówków wiadomości.
 - 5.27.2.4. Możliwość podpisywania treści wiadomości (ang. Body) bez limitu rozmiaru wiadomości albo z ustaleniem jaki rozmiar wiadomości zostanie podpisany
- 5.28. W ramach oferowanego systemu należy zapewnić rozwiązanie do centralnej, wspólnej obsługi kwarantanny ze wszystkich działających w sieci *appliance*.
- 5.29. Interfejs zarządzający musi umożliwiać administratorowi zarządzanie wiadomościami przechowywanymi w centralnej kwarantannie.
- 5.30. Decyzja o przesłaniu wiadomości do kwarantanny musi wynikać z definicji działania poszczególnych filtrów: antywirusowego, antyspamowego lub weryfikacji treści.
- 5.31. System SOSZ musi umożliwiać tworzenie wielu kont administracyjnych z różnym poziomem uprawnień (role).
- 5.32. Jeżeli system SOSZ nie wykorzystuje mechanizmów autoryzacji Active Directory, musi zapewniać odpowiedni poziom ochrony haseł dla kont tworzonych w systemie.
- 5.33. Rozwiązanie musi pozwalać na logowanie aktywności użytkowników systemu - zakres logów powinien być zgodny z aktualnymi wymaganiami wskazanymi w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz norm PN-ISO/IEC 27001 i PN-ISO/IEC 27002.
- 5.34. Rozwiązanie musi posiadać wbudowane mechanizmy pozwalające na wysyłanie powiadomień o stanie pracy poszczególnych komponentów systemu, w tym SNMP.

- 5.35. System musi zapewniać możliwość monitorowania jego wydajności przez protokół SNMP w wersji 2c i 3.
- 5.36. System musi być kompatybilny z otwartym standardem REST API/ICAP posiadanego przez Zamawiającego *sandbox'a* w celu analizy próbki.
- 5.37. System SOSZ musi pozwalać na integrację z systemem analizy zagrożeń typu *on-premise Sandbox*. Integracja powinna polegać co najmniej na możliwości automatycznego wysyłania do analizy podejrzanych wiadomości, w tym załączników wg zdefiniowanych polityk.
- 5.38. System SOSZ musi pozwalać na automatyczne wysyłanie logów do sysloga (SIEM)

Wymagania funkcjonalne w zakresie ochrony antywirusowej

- 5.39. System SOSZ musi być wyposażony w co najmniej jeden skaner AV (antywirusowy). Jeden skaner AV musi pochodzić od tego samego producenta, co całe oferowane rozwiązanie.
- 5.40. Skaner AV musi wykorzystywać, automatyczne aktualizacje baz sygnatur antywirusowych. Musi istnieć możliwość określenia częstotliwości i harmonogramu aktualizacji silnika AV i baz sygnatur. Zapytania o dostępność nowych aktualizacji sygnatur antywirusowych muszą odbywać się na bieżąco, nie rzadziej niż co godzinę, a co najmniej raz dziennie wymagana jest aktualizacja sygnatur.
- 5.41. Skaner AV musi posiadać mechanizm wykrywający nowe zagrożenia za pomocą internetowych serwisów reputacyjnych zarządzanych przez producenta rozwiązania. W razie wykrycia podejrzanego kodu/pliku i braku definicji w lokalnym pliku sygnatur antywirusowych, skaner AV musi mieć możliwość wysłania zapytania do centralnej bazy prowadzonej przez producenta.
- 5.42. Skaner AV musi wykrywać i blokować oprogramowanie szpiegujące oraz wykrywać próby ataków typu *phishing*.
- 5.43. Skaner AV musi wykrywać wykorzystanie mechanizmów kompresji używanych przez szkodliwe oprogramowanie i musi umożliwiać automatyczne skasowanie plików przygotowanych z ich użyciem.
- 5.44. Skaner AV musi umożliwiać blokowanie skryptów, apletów Java oraz ActiveX.

Wymagania funkcjonalne w zakresie ochrony antyspamowej

- 5.45. System SOSZ musi zapewniać ochronę przed spamem – powinien być wyposażony w moduł antyspamowy (AS) pochodzący od tego samego producenta, co całe oferowane rozwiązanie.
- 5.46. Skaner AS musi działać w oparciu o system oceny prawdopodobieństwa wystąpienia spamu bazujący na regułach aktualizowanych przez producenta.
- 5.47. Zapytania o dostępność nowych aktualizacji sygnatur antyspamowych muszą odbywać się na bieżąco, nie rzadziej niż co godzinę, a co najmniej raz dziennie wymagana jest aktualizacja sygnatur
- 5.48. System AS musi mieć możliwość wysyłania zapytania do internetowego serwisu reputacyjnego producenta w celu dalszej weryfikacji dodatkowymi mechanizmami antyspamowymi.
- 5.49. Skaner AS musi współpracować z serwerami AD DS i LDAP, posiadanymi przez Zamawiającego, pozwalając na stworzenie polityki skanowania zależnie od adresu pocztowego, grupy użytkowników w AD DS/LDAP, domeny pocztowej lub zakresu IP.
- 5.50. System AS musi obsługiwać białe i czarne listy (*blacklist* i *whitelist*) definiowane przez administratora.
- 5.51. System AS musi obsługiwać serwery RBL zarządzane przez producenta rozwiązania. Powinno być także możliwe definiowanie dodatkowych źródeł RBL przez administratora systemu.
- 5.52. System ma zapewniać ochronę *anti-open-relay*.
- 5.53. System AS musi wykrywać i blokować ataki typu *directory harvest*.
- 5.54. System AS musi obsługiwać technologie: *graylisting*, SPF, DKIM. Weryfikacja sygnatury DKIM w wiadomościach. Moduł musi obsługiwać klucze DKIM o długości przynajmniej 2048 bity.

- 5.55. System AS musi chronić przed spamem generowanym za pomocą mechanizmu potwierdzania problemów z doręczeniem przesyłki (NDR).
- 5.56. System powinien wykorzystywać funkcję FCrDNS realizującą sprawdzenie poprawności konfiguracji rozwiązywania nazw DNS systemu nadającego wiadomość.
- 5.57. System AS musi posiadać filtr reputacyjny badający domenę i adres IP, z których nadana została wiadomość oraz zawartość przesyłaną w email.
- 5.58. System AS musi posiadać ochronę przed zagrożeniami typu *business email compromise* (BEC)
- 5.59. Musi być możliwe takie skonfigurowanie polityki ochrony antyspamowej, aby już sam wynik z serwisu reputacyjnego (niska reputacja nadawcy) powodował odrzucenie email lub skierowanie go do kwarantanny.
- 5.60. System musi umożliwiać badanie reputacji URL w treści wiadomości i filtrować wiadomość z URL o złej reputacji.
- 5.61. System musi umożliwiać „rozbrojenie” adresu URL w wiadomości email, w przypadku braku jednoznacznej, pozytywnej jego oceny przez serwis reputacyjny lub braku takiej oceny poprzez co najmniej przekształcenie go do postaci „nieklikalnej” lub wygenerowanie dodatkowego ostrzeżenia np. poprzez przekierowanie adresu URL do usługi inspekcji adresów URL.
- 5.62. System musi sprawdzać w przychodzących wiadomościach email zgodność adresów nadawcy email kopertowego i nagłówkowego.
- 5.63. Musi być możliwe zdefiniowanie różnych akcji podejmowanych po wykryciu spamu zależnie od określonego przez system prawdopodobieństwa wykrycia spamu (*spam score*):
 - 5.63.1. Zablokowanie i skasowanie wiadomości z powiadomieniem końcowego użytkownika, a także bez takiego powiadomienia (zależnie od przyjętej polityki).
 - 5.63.2. Przekazanie wiadomości do kwarantanny.
 - 5.63.3. Przesłanie wiadomości do odbiorcy z oznakowaniem jej jako spam w tytule wiadomości.
 - 5.63.4. Dodanie do nagłówka wiadomości informacji o prawdopodobieństwie wystąpienia spamu.
 - 5.63.5. Dodanie do nagłówka wiadomości informacji, które reguły antyspamowe spowodowały wykrycie spamu.

Wymagania projektowe i szczegółowa specyfikacja prac

W ramach przedmiotu umowy Wykonawca wykona następujące prace:

- 5.64. Wdroży i skonfiguruje według zaakceptowanego Projektu technicznego dostarczone oprogramowanie oraz maszyny wirtualne typu VA lub *appliance* sprzętowe do ochrony zewnętrznych serwerów pocztowych.
- 5.65. Wykona niezbędną konfigurację sieciową i integrację z systemem pocztowym Zamawiającego.
- 5.66. Dokona migracji lub wymiany komponentów obecnego używanego systemu ochrony poczty korporacyjnej Zamawiającego.
- 5.67. Skonfiguruje polityki konfiguracyjne z wykorzystaniem najlepszych praktyk producenta oprogramowania dla wdrożonych produktów oraz z wykorzystaniem polityk z istniejącego rozwiązania.
- 5.68. Dokona integracji z *sandbox'em*
- 5.69. Opracuje scenariusze testowe i przeprowadzi testy akceptacyjne wdrożonego rozwiązania.
- 5.70. Opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy.

Dostawa i wdrożenie sprzętu typu *appliance*

- 5.71. Zamawiający wymaga, w przypadku zaoferowania fizycznych urządzeń, dostarczenia sprzętu:

- 5.71.1. fabrycznie nowego, nie używanego wcześniej w innych projektach (nie dopuszcza się rozwiązań typu „refurbished” itp.)
- 5.71.2. objętego 3 letnią opieką gwarancyjną, uwzględniającą aktualizacje oprogramowania/sterowników
- 5.71.3. pochodzącego z autoryzowanego kanału sprzedaży producentów zaoferowanych urządzeń,
- 5.71.4. nieprzeznaczonego, w dniu składania ofert, przez producenta do wycofania z produkcji,
- 5.71.5. współpracującego z siecią energetyczną o parametrach: 230 V \pm 10%, 50 Hz, jednofazowo i wyposażonego w przewody zasilające,
- 5.71.6. posiadającego najnowszą dostępną w dniu składania ofert wersję oprogramowania
- 5.72. Wykonawca w treści złożonej oferty oświadczy, że Urządzenia dostarczone Zamawiającemu będą spełniały powyższe wymagania.
- 5.73. Zamawiający wymaga w przypadku dostarczenia fizycznych urządzeń, aby sprzęt typu *appliance*:
 - 5.73.1. spełniał przewidziane przez producenta rozwiązania parametry techniczne z uwzględnieniem wymagań określonych przez Zamawiającego,
 - 5.73.2. był wyposażony w redundantne zasilacze,
 - 5.73.3. był wyposażony w redundantne interfejsy sieciowe.
- 5.74. Zaoferowany sprzęt typu *appliance*, musi być przystosowany do instalacji w posiadanych przez Zamawiającego szafach rack 19 cali.
- 5.75. Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) oraz niezbędny do jego prawidłowego podłączenia z dedykowaną siecią energetyczną Zamawiającego o parametrach: 230V \pm 10%, 50Hz oraz siecią logiczną. W szafach rack Zamawiającego są dostępne listwy zasilające z gniazdami C13 lub istnieje możliwość dedykowanego zasilania.
- 5.76. Wszystkie dostarczane urządzenia muszą zawierać sieciowe okablowanie logiczne. Zamawiający udostępni przełączniki sieciowe w architekturze programowalnej SDN (ang. Software Defined Network) z wykorzystaniem urządzeń i technologii firmy Cisco ACI Version: 4.2(2g) do podłączenia Systemu poprzez interfejsy fizyczne miedziane RJ45 lub światłowodowe w standardzie SFP/SFP+ 1Gbps oraz 10Gbps. Wykonawca dostarczy do posiadanych przez Zamawiającego przełączników sieciowych Cisco N9K-C93180YC-FX odpowiednią ilość kompatybilnych **wkładek**, nie powodujących utraty gwarancji producenta na te przełączniki, niezbędnych do prawidłowego funkcjonowania systemu oraz kable umożliwiające włączenie dostarczonych urządzeń do infrastruktury sieciowej Zamawiającego opartej na w/w typie przełączników.
- 5.77. Wykonawca gwarantuje, że wszystkie dostarczane produkty (dotyczy to zarówno sprzętu jak i oprogramowania) są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca.
- 5.78. Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów użytkowania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej).
- 5.79. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. Zamawiający wymaga, aby urządzenia były rozpakowane i uruchomione wyłącznie przez Wykonawcę lub podmioty przez niego uprawnione.
- 5.80. Dostawa sprzętu i oprogramowania zostanie zrealizowana zgodnie z wymaganiami:
 - 5.80.1. Wykonawca dostarczy całość sprzętu wraz z oprogramowaniem do siedziby Zamawiającego.
 - 5.80.2. Wykonawca dostarczy sprzęt w dni robocze od poniedziałku do piątku.

- 5.80.3. Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do serwerowni w budynku GUS, które są zlokalizowane na parterze oraz na pierwszym piętrze.
- 5.81. Wszystkie prace instalacyjne oraz wdrożeniowe będą uzgadniane i realizowane we współpracy z administratorami Zamawiającego.
- 5.82. Montaż sprzętu, podłączenie okablowania, instalacja oprogramowania oraz inne czynności konieczne do uruchomienia przedmiotu zamówienia, zostaną wykonane przez Wykonawcę w ramach ceny za przedmiot zamówienia.
- 5.83. Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty przedmiotu zamówienia zgodnie z opracowanym Projektem Technicznym Systemu.
- 5.84. Wykonawca dostarczy licencje oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację systemu w infrastrukturze IT Zamawiającego i zostały określone ilościowo i jakościowo w projekcie technicznym Systemu.
- 5.85. Wykonawca zainstaluje dostarczane urządzenia w serwerowni GUS w posiadanych przez Zamawiającego szafach rack 19".
- 5.86. Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, patchcords - kable Ethernet kat. 6, bezpieczniki, gniazda zasilające, moduły PDU do szaf rack, organizery okablowania, peszle itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń dostarczanych w ramach przedmiotowego postępowania zgodnie z opracowanym Projektem Technicznym Systemu.
- 5.87. Wykonawca wykona konieczne połączenia sieciowego okablowania logicznego pomiędzy dostarczonymi urządzeniami, a przełącznikami sieciowymi zamontowanymi w serwerowni Zamawiającego.
- 5.88. Wykonawca oznaczy każdy kabel w sposób umożliwiający jego jednoznaczną identyfikację zgodnie z przyjętą przez Zamawiającego konwencję nazewnictwa.
- 5.89. Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zgodny z obowiązującymi przepisami, zapewniający właściwe bezpieczeństwo użytkowania.
- 5.90. Jeżeli będzie to konieczne, Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania.
- 5.91. Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, peszlach, organizerach okablowania.
- 5.92. Wszystkie nośniki danych dostarczane wraz z urządzeniami pozostają w siedzibie Zamawiającego i przechodzą na jego własność. Wykonawca dostarczy na płytach CD/DVD lub pamięci Flash (pendrive) komplet sterowników systemowych i niezbędne oprogramowanie narzędziowe producenta.
- 5.93. Wykonawca jest zobowiązany do posprzątania i wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania.
- 5.94. Wykonawca dokona uruchomienia i wstępnej konfiguracji dostarczanego sprzętu wraz z oprogramowaniem w infrastrukturze IT zgodnie z opracowanym Projektem Technicznym Systemu.
- 5.95. Wykonawca dokona aktualizacji oprogramowania firmware, wszystkich dostarczonych urządzeń do najnowszych stabilnych wersji.

Procedura odbiorcza Zadania 2.

- 5.96. Dostawa i dokonanie wdrożenia systemu SOSZ przez Wykonawcę, potwierdzone zostanie podpisaniem z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokołem odbioru Zadania 2.

6. Zadanie 3: Dostawa oraz wdrożenie oprogramowania do zabezpieczenia wewnętrznych serwerów pocztowych wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSW (Systemem ochrony serwerów wewnętrznych)

Przedmiotem zadania jest dostawa oraz wdrożenie oprogramowania wraz z licencjami oraz trzyletnim wsparciem producenta pozwalającym na pobieranie aktualnych baz sygnatur wirusów, instalację nowych wersji oprogramowania i korzystanie z pomocy technicznej, dla 6500 użytkowników lub 7000 skrzynek pocztowych..

Wymagania ogólne w zakresie licencji

- 6.1. Licencje mogą być dostarczone w pakiecie zawierającym różne funkcjonalności lub jako samodzielne produkty, muszą pochodzić od tego samego producenta. Zamawiający wymaga trzyletniego wsparcia producenta na zamawiane oprogramowanie. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy serwerami pocztowymi.
- 6.2. Zamawiający wymaga aby terminem rozpoczęcia biegu dostarczonych licencji był 1 stycznia 2025. Jeżeli na czas wdrożenia i migracji systemu wymagane jest objęcie licencją systemu SOSW, Zamawiający wymaga dostarczenia dodatkowych licencji przejściowych (np. testowych).

Wymagania funkcjonalne

- 6.3. Dostarczone rozwiązanie ma obsługiwać 6500 użytkowników lub 7000 skrzynek pocztowych skrzynek pocztowych Zamawiającego.
- 6.4. Ochrona ma być realizowana przez dedykowane oprogramowanie antywirusowe instalowane na platformie serwerów MS Exchange 2019 analizujące wiadomości pocztowe przyjmowane przez te serwery.
- 6.5. System SOSW musi zawierać co najmniej jeden skaner antywirusowy inny (innego producenta) niż używany w SOSZ.
- 6.6. System SOSW musi być zgodny z MS Exchange 2019 posiadanym przez Zamawiającego (zgodnie z opisem środowiska Zamawiającego).
- 6.7. System SOSW musi się integrować z systemem poczty elektronicznej MS Exchange 2019 z wykorzystaniem przewidzianych przez twórców oprogramowania Exchange do tego celu mechanizmów (interfejsów programowych) - Transport Agent.
- 6.8. Ochroną antywirusową objęta musi być poczta elektroniczna Zamawiającego na wszystkich etapach transmisji przesyłki pocztowej:
 - 6.8.1. Na etapie przyjmowania/wysyłania przesyłki pocztowej z/do Internetu – na serwerach MS Exchange Edge Server Role.
 - 6.8.2. Na etapie transportu przesyłki pocztowej - na serwerach MS Exchange Mailbox Server Role.
 - 6.8.3. Na etapie składowania przesyłki pocztowej - na serwerach MS Exchange Mailbox Server Role.
- 6.9. Sprawdzane antywirusowo muszą być przesyłki zarówno przychodzące jak i wychodzące do/z skrzynki pocztowej użytkownika.
- 6.10. Sprawdzanie antywirusowe przesyłek na serwerach transportowych poczty elektronicznej (MS Exchange Edge Server Role) musi odbywać się w czasie rzeczywistym nie zakłócając prawidłowego przebiegu przesyłki pocztowej, wykorzystując funkcjonalność *Transport Agent*.
- 6.11. Sprawdzanie antywirusowe przesyłek na serwerach skrzynkowych (MS Exchange Mailbox Server Role) musi się odbywać bezpośrednio w storach Exchange:
 - 6.11.1. W momencie dotarcia przesyłki pocztowej na serwer skrzynkowy.
 - 6.11.2. W momencie pojawienia się nowoutworzonej, przez użytkownika, przesyłki pocztowej.
 - 6.11.3. Zgodnie z harmonogramem sprawdzania skrzynek pocztowych użytkowników.
 - 6.11.4. Na żądanie administratora systemu antywirusowego poczty elektronicznej.

- 6.12. W przypadku wykrycia szkodliwego pliku/kodu musi istnieć możliwość usunięcia wiadomości/załącznika, wyleczenia, podmiany załącznika na czysty plik zawierający jedynie informację o infekcji.
- 6.13. W przypadku wykrycia szkodliwego pliku/kodu wiadomości system musi generować powiadomienia dla administratora systemu.
- 6.14. Przesyłki, w których wystąpiło podejrzenie występowania szkodliwej zawartości muszą być składowane w miejscu niedostępnym dla użytkowników poczty (w kwarantannie).
- 6.15. Administrator systemu antywirusowego poczty elektronicznej musi mieć możliwość zarządzania kwarantanną poprzez:
 - 6.15.1. Wgląd do zawartości kwarantanny.
 - 6.15.2. Usuwanie przesyłek z kwarantanny.
 - 6.15.3. Zwalnianie przesyłek z kwarantanny – skierowanie przesyłki wcześniej poddanej kwarantannie do adresata.
 - 6.15.4. Mechanizm kwarantanny musi mieć zabezpieczenie przed przepełnieniem.
- 6.16. System SOSW musi być zarządzany z jednego miejsca – za pomocą centralnej konsoli administracyjnej.
- 6.17. System SOSW musi wspierać rozwiązania klastrowe DAG.
- 6.18. Oprogramowanie musi korzystać z dziennych uaktualnień sygnatur. Oprogramowanie powinno sprawdzać pojawienie się nowych sygnatur przynajmniej 4 razy dziennie.
- 6.19. System ochrony poczty elektronicznej SOSW może zawierać dodatkowe funkcjonalności (np. ochronę antyspamową, *anti-ransomware*, *anti-phishing* itp.), jeżeli wchodzi w skład zaproponowanego pakietu oprogramowania. Obecność tych funkcjonalności nie jest wymagana.

Wymagania projektowe i szczegółowa specyfikacja prac

W ramach przedmiotu umowy Wykonawca wykona następujące prace:

- 6.20. Wdroży i skonfiguruje dostarczone oprogramowanie do ochrony wewnętrznych serwerów pocztowych.
- 6.21. Dokona migracji lub wymiany komponentów obecnego używanego systemu ochrony poczty korporacyjnej Zamawiającego.
- 6.22. Skonfiguruje polityki konfiguracyjne z wykorzystaniem najlepszych praktyk producenta oprogramowania dla wdrożonych produktów.
- 6.23. Opracuje scenariusze testowe i przeprowadzi testy akceptacyjne wdrożonego rozwiązania.
- 6.24. Opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy.

Procedura odbiorcza Zadania 3.

- 6.25. Dostawa i dokonanie wdrożenia systemu SOSW przez Wykonawcę, potwierdzone zostanie podpisaniem z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokołem odbioru Zadania 3.

7. **Zadanie 4:** Wykonanie dokumentacji powykonawczej i przeprowadzenie warsztatów

Dokumentacja powykonawcza

Wykonawca opracuje kompleksową Dokumentację powykonawczą całego rozwiązania dostarczonego

w ramach opisanych w OPZ zadań, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje istotne w eksploatacji dostarczonego rozwiązania. Dokumentacja powykonawcza w szczególności będzie zawierać:

- 7.1. Opis architektury zaimplementowanego rozwiązania.
- 7.2. Szczegółowy opis instalacji i konfiguracji wykorzystywanego oprogramowania, ze wskazaniem wybranych opcji i ustawionych wartości. Konfigurację poszczególnych modułów, komponentów i usług.
- 7.3. Zbiór zaimplementowanych polityk konfiguracyjnych dla poszczególnych modułów.
- 7.4. Politykę i procedury wykonywania i przechowywania kopii zapasowych oraz ich testowania i odtwarzania.
- 7.5. Szczegółowe procedury eksploatacyjne oraz awaryjnego odtwarzania funkcjonalności systemu, opisujące krok po kroku niezbędne czynności umożliwiające Zamawiającemu samodzielne przywrócenie funkcjonalności systemu.
- 7.6. Procedury i instrukcje bieżącego monitoringu oraz utrzymania i aktualizacji systemu.
- 7.7. Instrukcje dla użytkowników/ administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa.
- 7.8. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z Zamawiającym
- 7.9. Jeżeli system wykorzystuje modele i algorytmy sztucznej inteligencji:
 - 7.9.1. Wykonawca zobowiązany jest do poinformowania Zamawiającego o tym fakcie oraz do przedstawienia szczegółowych informacji dot. ich działania, w tym w jakim module/funkcjonalności zostały wykorzystane oraz jakie są zasady ich działania;
 - 7.9.2. Zamieszczenia w dokumentacji powykonawczej ich dokładnego opisu;
 - 7.9.3. Wykonawca bierze pełną odpowiedzialność za ich prawidłowe działanie;
 - 7.9.4. W okresie świadczonej gwarancji Wykonawca udzieli profesjonalnego wsparcia w zakresie wykorzystania tych funkcjonalności, w szczególności w zakresie: audytu poprawek, wykonywania aktualizacji oprogramowania, testowania konfiguracji oprogramowania, transferu wiedzy;
 - 7.9.5. Wykonawca musi zapewnić, że ich użycie jest w pełni konfigurowalne tj. Zamawiający będzie miał możliwość dowolnego wyłączenia i włączenia tych mechanizmów, a ich wyłączenie nie wpłynie na prawidłowość działania systemu i nie będzie skutkowało brakiem spełnienia przez system wymagań OPZ.
- 7.10. Wykonawca zobowiązany jest umieścić w dokumentacji powykonawczej zakres informacji jakie są przekazywane do serwisów reputacyjnych producenta w czasie działania systemu.

Zamawiający wymaga, aby Dokumentacja powykonawcza napisana była w języku polskim. Wykonawca przekaże Zamawiającemu Dokumentację powykonawczą w trzech egzemplarzach w formie papierowej oraz w formie elektronicznej na nośniku CD lub na nośniku pamięci flash (pendrive). Dokumentacja na nośniku musi posiadać format pliku do edycji.

Warsztaty

Wykonawca w ramach ceny za przedmiot zamówienia przeprowadzi dwa warsztaty on-line dla 6 osób, trwające:

- 7.11. Warsztaty dla administratorów systemu ochrony zewnętrznych serwerów pocztowych: 6 osób, czas trwania szkolenia: 3 dni robocze (24 godziny zegarowe),
- 7.12. Warsztaty dla administratorów systemu ochrony wewnętrznych serwerów pocztowych: 6 osób, czas trwania szkolenia: 2 dni robocze (16 godzin zegarowych),

- 7.13. Opracuje materiał warsztatowy, w formie skryptu, w języku polskim w wersji elektronicznej i udostępni dla każdego uczestnika.
- 7.14. Zakres warsztatów będzie obejmował zagadnienia dotyczące Systemu – instalacja i konfiguracja komponentów wdrożonego rozwiązania ze szczególnym uwzględnieniem konfiguracji polityk poszczególnych modułów oraz aktualizacja, backup, *troubleshooting*, integracja z innymi rozwiązaniami, dobre praktyki i reakcja na zdarzenia.
- 7.15. Warsztaty zostaną zrealizowane w terminie uzgodnionym przez strony umowy, jednak nie później niż do końca lutego 2025.
- 7.16. Warsztaty zostaną przeprowadzone zdalnie, z dostępem do wdrożonego systemu lub w inny uzgodniony przez upoważnione do realizacji przedmiotu zamówienia osoby. Wykonawca zobowiązany jest do zapewnienia odpowiednich rozwiązań teleinformatycznych na potrzeby przeprowadzania warsztatów.
- 7.17. Warsztaty zostaną przeprowadzone przez osoby mające profesjonalną (zawodową) wiedzę z zakresu przedmiotu zamówienia.
- 7.18. Na początku warsztatów Wykonawca poinformuje uczestników, że po zakończeniu warsztatu zostaną poproszeni o elektroniczne wypełnienie arkuszy AIOS (Ankieta Indywidualnej Oceny Szkolenia), co ma na celu zebranie informacji na temat jakości warsztatów. Niedopuszczalne jest sugerowanie uczestnikom odpowiedzi na pytania zawarte w arkuszu.
- 7.19. Na koniec warsztatów Wykonawca przekaże do wypełnienia każdemu uczestnikowi Arkusz AIOS, w postaci dokumentu elektronicznego. Na podstawie wypełnionych elektronicznie i przesłanych Arkuszy AIOS Wykonawca przygotuje zbiorcze zestawienie zawierające analizę danych zawartych w ankietach, obrazującą stopień zadowolenia uczestników oraz użyteczność przeprowadzonego warsztatu. W terminie do 2 dni roboczych od dnia przeprowadzenia warsztatów, Wykonawca przekaże, w formie elektronicznej, Zamawiającemu wypełnione przez uczestników Arkusze AIOS wraz ze zbiorczym zestawieniem ocen z Arkuszy AIOS. W przypadku negatywnej oceny warsztatu (średnia z oceny trenera / trenerów poniżej 3) lub przeprowadzenia warsztatów niezgodnie z wymaganiami Zamawiającego, Wykonawca przeprowadzi dodatkowe warsztaty, dochowując terminu realizacji zamówienia. Organizacja dodatkowej edycji warsztatów będzie wymagała uzgodnienia z Zamawiającym terminu oraz osoby prowadzącej. Ponowne przeprowadzenie warsztatów musi się odbyć nie później niż 10 dni przed terminem zakończenia Zadania 2. Koszt ponownego zorganizowania i przeprowadzenia warsztatów ponosi Wykonawca.
- 7.20. Wykonawca po zakończeniu warsztatów przekaże Zamawiającemu, przygotowane w formie papierowej, wydane dla każdego uczestnika imienne zaświadczenie o ukończeniu warsztatów, które będzie zawierało następujące informacje: imię i nazwisko uczestnika, tytuł warsztatów, liczbę godzin, tematykę i datę przeprowadzenia warsztatów, pieczęć Wykonawcy, identyfikowalny podpis osoby prowadzącej warsztaty. Warunkiem wydania zaświadczenia jest:
- 7.20.1. potwierdzona obecność uczestnika w każdym dniu zajęć poprzez dokonane online przez uczestnika zgłoszenie uczestnictwa,
- 7.20.2. przesłanie przez uczestnika wypełnionego elektronicznie arkusza AIOS.
- 7.21. W terminie 2 dni od dnia zakończenia warsztatów, Wykonawca przekaże Zamawiającemu na adres poczty elektronicznej, zeskanowane w formacie PDF wypełnione arkusze AIOS oraz dokumenty potwierdzające uczestnictwo osób biorących udział w warsztatach, w każdym z trzech dni zajęć, w postaci *printscreen'a* z platformy, na której uczestnicy szkolenia byli zalogowani.
- 7.22. Potwierdzeniem zrealizowania warsztatu, będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokół odbioru warsztatów
- 7.23. Protokół odbioru warsztatów w formie papierowej, Wykonawca dostarczy Zamawiającemu w terminie 4 dni roboczych od zakończenia warsztatów

Procedura odbiorcza Zadania 4.

- 7.24. Dokumentacja Powykonawcza podlegała będzie procedurze odbioru, na następujących warunkach:

- 7.24.1. Wykonawca prześle Zamawiającemu drogą elektroniczną do akceptacji dokumentację powykonawczą, co najmniej na 10 dni roboczych przed terminem zakończenia realizacji umowy;
 - 7.24.2. Zamawiający w terminie nie dłuższym niż 3 dni od dnia dostarczenia przez Wykonawcę dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
 - 7.24.3. Wszystkie uwagi do dokumentacji powykonawczej zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 2 dni robocze od dnia ich otrzymania;
 - 7.24.4. Zamawiający w terminie 2 dni robocze od dnia powtórnego dostarczenia przez Wykonawcę poprawionej dokumentacji powykonawczej, poinformuje Wykonawcę o jej akceptacji lub konieczności wprowadzenia zmian;
 - 7.24.5. Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w dokumentacji powykonawczej;
 - 7.24.6. W przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo wskazania ostatecznego terminu dostarczenia dokumentacji nie dłużej niż 5 dni, w przeciwnym razie Zamawiający ma prawo do odstąpienia od Umowy i przekazanie wykonawstwa firmie trzeciej na koszt i ryzyko Wykonawcy;
 - 7.24.7. Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji Dokumentacji Powykonawczej, następować będzie drogą mailową na adresy Wykonawcy i Zamawiającego wskazane w umowie;
 - 7.24.8. Zatwierdzona Dokumentacja Powykonawcza zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu Odbioru Dokumentacji Powykonawczej na pendrive w wersji edytowalnej i PDF oraz wydruk papierowy w 2 egzemplarzach,
- 7.25. Zadanie 4 zostaje zakończone po podpisaniu Protokołu Odbioru Zadania 4 bez zastrzeżeń.

8. Gwarancja

- 8.1. Zamawiający wymaga, aby wszystkie dostarczone komponenty Systemu, w ramach ceny za przedmiot zamówienia, były objęte opieką gwarancyjną na okres 3 lat.
- 8.2. Termin biegu gwarancji liczony będzie od dnia podpisania z wynikiem pozytywnym. Protokołu odbioru Zadania 3 lub Protokołu odbioru Zadania 2 w zależności co nastąpi później.
- 8.3. W ramach gwarancji na wdrożony system zapewni,;
 - 8.3.1. usuwanie wad konfiguracyjnych wdrożonego;
 - 8.3.2. przywracanie pełnej funkcjonalności działania komponentów systemu, jeżeli ich niewłaściwe działanie bądź awaria wynika z instalacji lub konfiguracji zrealizowanych podczas wdrożenia;
- 8.4. Wykonawca zapewni, w okresie trwania umowy, 100 bezpłatnych godzin asysty technicznej, w ramach której świadczyć będzie następujące usługi, w przypadku ich wystąpienia
 - 8.4.1. konsultacje w zakresie konfiguracji i eksploatacji systemu;
 - 8.4.2. pomoc w rozwiązywaniu problemów technicznych związanych z funkcjonowaniem powstałego systemu;
 - 8.4.3. rozbudowę lub modyfikację systemu;
- 8.5. Usługi asysty technicznej oraz opieki gwarancyjnej, zlecane będą, w miarę potrzeb Zamawiającego, drogą elektroniczną na adres poczty elektronicznej wskazany przez Wykonawcę.
- 8.6. Wykorzystanie liczby godzin asysty technicznej będzie dokumentowane, sporządzanym raz na 12 miesięcy, Protokołem odbioru asysty technicznej.

- 8.7. W przypadku konieczności zmiany Dokumentacji powykonawczej, w wyniku dokonania istotnych zmian konfiguracyjnych, Wykonawca zobowiązany jest dostarczyć zaktualizowaną dokumentację w terminie 30 dni roboczych po ich wykonaniu.
- 8.8. Wykonawca zobowiązuje się do świadczenia gwarancji na następujących zasadach:

Problem	Czas reakcji (godziny)	Czas przywrócenia systemu lub rozwiązanie zastępcze (godziny)	Czas naprawy - rozwiązania problemu (godziny)
Awaria krytyczna	4	24	48
Błąd	8	-	96

- 8.9. Problemy objęte gwarancją będą klasyfikowane, jako Awarie krytyczne i Błędy w następujący sposób:
- 8.9.1. Awaria krytyczna: to sytuacja, w której brak jest możliwości użytkowania, co najmniej jednego z urządzeń Systemu.
- 8.9.2. Błąd: sytuacja, której skutkiem jest brak możliwości użytkowania komponentu lub funkcjonalności Systemu.
- 8.9.3. Czas reakcji rozumiany, jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem problemu do Serwisu Wykonawcy a czasem rozpoczęcia działań zmierzających do naprawy (wyeliminowania) zgłoszonego problemu.
- 8.9.4. Czas przywrócenia systemu lub rozwiązania zastępczego problemu – czas liczony od momentu zgłoszenia, po którym rozwiązanie problemu, które może być realizowane poprzez zmianę parametrów Systemu, rekomendację modyfikacji procesu przetwarzania danych, rekomendację modyfikacji sprzętowo-programowej, rekomendację modyfikacji infrastruktury wykorzystywanej przez System lub inne rekomendacje prowadzące do zmiany kategorii problemu na niższą bądź do zamknięcia problemu – naprawy (rozwiązanie końcowe).
- 8.9.5. Czas naprawy - rozwiązania problemu – maksymalny czas, po którym musi zostać przywrócona pełna funkcjonalność Systemu, liczony od momentu zgłoszenia.
- 8.9.6. Zastosowanie Rozwiązania zastępczego nie zwalnia Wykonawcy z obowiązku dostarczenia dla niego właściwego rozwiązania końcowego.
- 8.10. Jeśli Błąd dotyczy Oprogramowania i Wykonawca uzyska diagnozę problemu wskazującą, że naprawa wymaga instalacji nowej wersji oprogramowania, Wykonawca zobowiązany jest przekazać Zamawiającemu treść diagnozy i zastosować rozwiązanie zastępcze problemu.
- 8.11. Na czas naprawy oprogramowania zostanie wstrzymany upływ Czasu Naprawy do czasu zainstalowania przez Wykonawcę nowej wersji oprogramowania wskazanej przez producenta Oprogramowania.
- 8.12. Serwis w ramach udzielonej gwarancji, świadczony będzie w języku polskim zdalnie poprzez środki komunikacji elektronicznej lub w siedzibie Zamawiającego.
- 8.13. Zgłaszanie problemów będzie możliwe przez 7 dni tygodnia w godzinach 0:00-24:00 w sposób uzgodniony z Wykonawcą.
- 8.13.1. podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nie może przekroczyć 4 godzin lub 8 godzin od momentu gwarancyjnego zgłoszenia przez Zamawiającego jeżeli do zgłoszenia doszło do godziny 16:00 dnia roboczego,
- 8.13.2. w przypadku gwarancyjnego zgłoszenia Awarii po godzinie 16:00 lub w dzień ustawowo wolny od pracy, podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nastąpi następnego dnia roboczego w godzinach od 8:00 do 12:00,

- 8.14. Zamawiający wymaga udostępnienia przez Wykonawcę Zamawiającemu, na jego prośbę, dostępu do informacji o zgłoszeniach.
- 8.15. Wykonawca przyjmie zgłoszenie i potwierdzi jego przyjęcie nie później niż do chwili upływu Czasu Reakcji, który wlicza się do Czasu rozwiązania problemu.
- 8.16. W razie wątpliwości uznaje się, że zgłoszenie zostało dokonane w chwili wysłania informacji w formie mailowej lub za pomocą dedykowanego narzędzia. Ryzyko nieotrzymania prawidłowo przekazanego zgłoszenia spoczywa na Wykonawcy, z wyjątkiem sytuacji, gdy Wykonawca udowodni, że nie otrzymał wiadomości z przyczyn od niego niezależnych.
- 8.17. Wskazane powyżej czasy liczone są od chwili dokonania zgłoszenia w sposób ciągły w odniesieniu do pojedynczego zgłoszonego problemu: Awarii lub Błędu.
- 8.18. Wszelkie koszty związane z naprawami, usuwaniem Problemu, włączając w to koszt części, usług i transportu z i do siedziby Zamawiającego ponosi Wykonawca.
- 8.19. W przypadku stwierdzenia niezgodności w sposobie realizacji przez Wykonawcę zobowiązań gwarancyjnych, Zamawiający zastrzega sobie prawo do naliczenia kar umownych i potrącenia ich z Zabezpieczenia należytego wykonania umowy.
- 8.20. W przypadku, jeżeli Wykonawca nie wywiązuje się ze zobowiązań wynikających z gwarancji, Zamawiający może dokonać naprawy konfiguracji we własnym zakresie lub zlecić jej wykonanie osobie trzeciej, a kosztami obciążyć Wykonawcę z wykorzystaniem kwoty zabezpieczenia należytego wykonania umowy.
- 8.21. Zamawiający ma prawo dokonywania modyfikacji konfiguracji przez przeszkolonych pracowników, zgodnie z Dokumentacją powykonawczą.
- 8.22. Wykonawca w okresie gwarancji jest zobowiązany co najmniej raz w roku od odbioru przedmiotu zamówienia, do wykonania wspólnie z Zamawiającym:
- 8.22.1. bezpłatnego przeglądu Systemu
 - 8.22.2. aktualizacji wymaganych lub rekomendowanych przez producenta lub producentów komponentów Systemu
 - 8.22.3. uruchomić nowe, dostępne w ramach aktualizacji funkcjonalności istotne dla bezpieczeństwa teleinformatycznego.
- 8.23. W okresie gwarancji Wykonawca zapewni bezpłatnie dostarczanie nowych wersji oprogramowania oraz publikowanych poprawek wraz z ich instalacją.
- 8.24. W przypadku kiedy dostarczony będzie sprzęt (appliance):
- 8.24.1. W przypadku awarii wymagającej wymiany sprzętu, Wykonawca dostarczy Zamawiającemu sprzęt wolny od wad, równoważny jakościowo i funkcjonalnie w ciągu 72 godzin od zgłoszenia problemu.
 - 8.24.2. W przypadku uszkodzenia dysku (nośnika pamięci), Wykonawca dostarczy nowy dysk wolny od wad równoważny jakościowo i funkcjonalnie.
 - 8.24.3. Dysk uszkodzony przechodzi na własność Zamawiającego.
- 8.25. W okresie udzielonej gwarancji Wykonawca będzie w sposób systematyczny, analizował i optymalizował do potrzeb Zamawiającego (zmieniał konfigurację, dopasowywał lub poprawiał) działanie Systemu i jego komponentów, w celu osiągnięcia możliwie najwyższych wskaźników wydajności i jakości działania.
- 8.26. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do stałego monitorowania podatności i luk bezpieczeństwa w systemie, w tym zobowiązuje się do prowadzenia okresowych lub na uzasadnione zlecenie Zamawiającego testów bezpieczeństwa i dostarczenia Zamawiającemu na jego żądanie, w terminie 2 dni od wykonania testu, raportów zawierających:
- 8.26.1. czynności wykonane w ramach testów,
 - 8.26.2. wykryte podatności wraz z określeniem ich poziomu istotności oraz wskazaniem jakie zagrożenie powodują
 - 8.26.3. wnioski oraz zalecenia dotyczące sugerowanych działań

8.26.4. wdrożone poprawki

- 8.27. Zamawiającemu przysługują niezależne prawa do przeprowadzania monitorowania podatności i luk bezpieczeństwa w systemie, w tym przeprowadzania testów bezpieczeństwa. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do współpracy z Zamawiającym w zakresie wykrytych przez Zamawiającego bądź podmiot trzeci podatności i luk w systemie oraz zobowiązuje się do niezwłocznego wprowadzania zmian i poprawek w systemie, które wynikać będą z rekomendacji po wykonanym teście, przy uwzględnieniu racjonalnych możliwości implementacji rekomendacji oraz przy uwzględnieniu, że ich wdrożenie nie naruszy praw autorskich do dostarczonego oprogramowania.
- 8.28. W okresie udzielonej gwarancji Wykonawca będzie współpracował z Zamawiającym w zakresie analizy raportów i testów bezpieczeństwa lub audytów systemów teleinformatycznych wykonanych niezależnie od przedmiotu umowy oraz wspierał obsługę i wprowadzanie koniecznych zmian i poprawek w Systemie wynikających z rekomendacji i możliwości implementacji, w zakresie w jakim nie narusza to praw autorskich do oprogramowania dostarczonego w ramach tego zamówienia.
- 8.29. Niezależnie od udzielonej gwarancji Zamawiającemu przysługuje rękojmia w zakresie przedmiotu zamówienia.