Załącznik nr 4 do ZO

**Opis Przedmiotu Zamówienia**

Przedmiotem zamówienia jest:

**„Świadczenie usługi poczty elektronicznej w modelu usługowym (SaaS) wraz z systemem ochrony klasy SEG (Secure Email Gateway) przez okres 36 miesięcy od dnia podpisania protokołu odbioru wdrożenia.”** w ramach projektu „Transformacja Cyfrowa Szpitala Miejskiego w Gliwicach Sp. z o.o. w ramach działania KPO - D.1.1.2” w ramach Krajowego Planu Odbudowy i Zwiększania Odporności – komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” - inwestycji D1.1.2 „ Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia”.

**1. Parametry Ogólne i Wydajność**

1. **Przedmiotem zamówienia jest świadczenie usługi poczty elektronicznej w modelu usługowym (SaaS) wraz z systemem ochrony klasy SEG (Secure Email Gateway) przez okres 36 miesięcy od dnia podpisania protokołu odbioru wdrożenia. Usługa musi być świadczona z wykorzystaniem infrastruktury sprzętowej fizycznie dedykowanej wyłącznie dla Zamawiającego.**
2. **Liczba kont: Minimum 2000 kont użytkowników (z opcją tworzenia nielimitowanej liczby skrzynek w ramach dostępnej przestrzeni).**
3. **Przestrzeń dyskowa: Łączna pojemność minimum 6 TB na dane pocztowe (nie licząc kopii zapasowych).**
4. **Skrzynka użytkownika: Minimalna pojemność 10 GB z opcją indywidualnego definiowania limitów przez administratora.**
5. **Obsługa domen: System musi obsługiwać domenę główną Zamawiającego oraz pozwalać na podpięcie wielu dodatkowych domen jako aliasów.**

**2. Dostęp i Interfejs Użytkownika**

1. **Protokoły: Pełna obsługa protokołów IMAP, SMTP oraz POP3 z obowiązkowym szyfrowaniem transmisji TLS/SSL. System musi zapewniać możliwość ograniczenia dostępu do tych protokołów wyłącznie ze wskazanych przez Zamawiającego adresów IP.**
2. **Webmail: Dedykowany interfejs przeglądarkowy w języku polskim z możliwością personalizacji wizualnej (logotyp Zamawiającego).**
3. **Uwierzytelnianie: Wymagane wieloskładnikowe uwierzytelnianie (2FA/MFA) dla dostępu przez interfejs przeglądarkowy. System musi umożliwiać wymuszenie stosowania drugiego składnika uwierzytelniania (np. TOTP) dla wszystkich logowań realizowanych spoza wskazanych przez Zamawiającego adresów IP (tzw. zaufanych lokalizacji sieciowych).**

**3. Bezpieczeństwo Sieciowe i Zgodność**

1. **Zgodność Prawna: System musi spełniać wymogi ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), dyrektywy NIS2 oraz RODO oraz wszelkich nowych regulacji i aktów wykonawczych z zakresu cyberbezpieczeństwa i ochrony danych, które wejdą w życie w okresie obowiązywania umowy.**
2. **Lokalizacja Danych: Przechowywanie i przetwarzanie danych wyłącznie na terenie Europejskiego Obszaru Gospodarczego (EOG).**
3. **Ochrona Brzegowa: Ochrona przed atakami DoS w warstwie 7 do 100 Gbps oraz monitorowanie infrastruktury przez system klasy SIEM.**
4. **Uwierzytelnianie Domeny: Pełna implementacja i weryfikacja rekordów SPF, DKIM oraz DMARC dla wszystkich wiadomości.**

**4. Zaawansowane mechanizmy filtrowania i ochrony Wykonawca zapewni dedykowaną warstwę ochrony poczty działającą przed serwerem docelowym, realizującą następujące funkcje:**

**1. Obiektowy system reguł: System musi pozwalać na definiowanie zaawansowanych polityk bezpieczeństwa w oparciu o hierarchiczny system reguł, umożliwiający tworzenie warunków logicznych łączących co najmniej następujące atrybuty:**

* **Atrybuty nadawcy i odbiorcy (adresy e-mail, domeny, grupy użytkowników/LDAP).**
* **Atrybuty zawartości (typy plików, nazwy załączników, treści nagłówków, wyrażenia regularne, wykrywanie spamu).**
* **Atrybuty czasowe (harmonogramy działania reguł).**
* **Atrybuty sieciowe (adresy IP źródłowe, geolokalizacja/GeoIP, strefy sieciowe).**

**2. Weryfikacja Techniczna i Anty-Spam: System musi posiadać zaimplementowane i aktywne następujące mechanizmy:**

* **Reverse DNS (rDNS): Obowiązkowa weryfikacja rekordu PTR nadawcy (odrzucanie połączeń z serwerów bez poprawnej konfiguracji DNS).**
* **Analiza URI (SURBL/URIBL): Wykrywanie spamu i phishingu w oparciu o analizę linków zawartych w treści wiadomości z wykorzystaniem baz reputacyjnych.**
* **Greylisting: Wsparcie dla mechanizmu Greylisting z możliwością definiowania wyjątków dla zaufanych nadawców.**
* **Analiza Nagłówków: Ochrona przed atakami typu spoofing poprzez analizę nagłówków i wykrywanie anomalii w polu "From" (niezgodność nadawcy kopertowego z nagłówkowym).**
* **Ochrona przed atakami słownikowymi: Mechanizm wykrywający i blokujący ataki typu "Dictionary Attack" oraz "Directory Harvest Attack" (DHA).**

**3. Weryfikacja Odbiorcy i Malware:**

* **Recipient Verification: Weryfikacja istnienia odbiorcy w czasie rzeczywistym na serwerze docelowym (poprzez protokół SMTP lub LDAP) w celu odrzucania błędnych wiadomości już na poziomie bramy.**
* **Antywirus: Skanowanie w czasie rzeczywistym wszystkich wiadomości (w tym analiza wnętrza archiwów ZIP/RAR/7Z).**

**5. Administracja i Monitorowanie**

1. **Panel Administratora: Dostęp przez HTTPS do zarządzania kontami, aliasami, grupami dystrybucyjnymi i białymi/czarnymi listami.**
2. **Śledzenie wiadomości (Tracking Center): Narzędzie umożliwiające podgląd drogi wiadomości i statusów SMTP w czasie rzeczywistym.**
3. **Logi: dostęp do logów pocztowych dla administratorów Zamawiającego.**

**6. Backup i Niezawodność (SLA)**

1. **SLA: Gwarantowana dostępność usługi na poziomie minimum 99,9% w skali roku. Zamawiający zastrzega, że minimalny gwarantowany czas dostępności usługi może być kryterium oceny w przetargu.**
2. **Backup: Pełna kopia zapasowa wykonywana minimum raz na dobę z okresem przechowywania 180 dni.**
3. **Zewnętrzna kopia: Możliwość automatycznego odkładania kopii zapasowej na zewnętrzny zasób wskazany przez Zamawiającego.**
4. **Wymóg separacji lokalizacji (Geo-redundancja): Ze względów bezpieczeństwa (ochrona przed skutkami zdarzeń losowych, np. pożar, zalanie, awaria zasilania w serwerowni), Zamawiający wymaga, aby kopie zapasowe były przechowywane w fizycznie odseparowanej lokalizacji (innym Centrum Przetwarzania Danych lub innej strefie dostępności chmury) względem infrastruktury podstawowej, na której świadczona jest usługa pocztowa. Infrastruktura zapasowa musi zapewniać możliwość odtworzenia danych w przypadku całkowitej niedostępności ośrodka podstawowego.**

**7. Migracja i Wsparcie**

1. **Zakres: Migracja obecnych danych (ok. 1 TB, IMAP, CardDav, listy mailingowe) w czasie do 7 dni. *W przypadku kontynuacji usługi u obecnego operatora, wymóg migracji uznaje się za spełniony, o ile infrastruktura spełnia wymogi OPZ.***
2. **Wsparcie: Helpdesk 24/7/365**
3. **Szkolenie: Szkolenie online dla min. 2 administratorów.**

**Szczegółowy przedmiot umowy określono w warunkach umowy, stanowiącej załącznik nr 2.**

**Przedmiot zamówienia musi zostać zrealizowany:**

**- do 15.04.2026 r.**

***Potwierdzam spełnienie zapisów Opisu przedmiotu zamówienia:***

„**Świadczenie usługi poczty elektronicznej w modelu usługowym (SaaS) wraz z systemem ochrony klasy SEG (Secure Email Gateway) przez okres 36 miesięcy od dnia podpisania protokołu odbioru wdrożenia.”**

|  |  |  |
| --- | --- | --- |
| …………………………………… | ……………………… | …………………………………………………………….. |
| Miejscowość | Data | *(podpis Wykonawcy lub osoby uprawnionej do jego reprezentowania)* |

***Dokument należy wypełnić elektronicznie. Zamawiający zaleca zapisanie dokumentu w formacie PDF (poprzez funkcję „zapisz jako”) i podpisanie podpisem kwalifikowanym lub podpisem zaufanym.***