



Dotyczy: **Zakup systemu bezpieczeństwa poczty elektronicznej wraz z rocznym wsparciem technicznym producenta**

Zawiadomienie o modyfikacji specyfikacji warunków zamówienia

ul. Zwycięstwa 21
44-100 Gliwice
tel. +48 32 231 30 41
fax +48 32 231 27 25
boi@um.gliwice.pl
www.gliwice.eu

Na podstawie art. 286 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, w imieniu zamawiającego informuję, że specyfikacja warunków zamówienia została zmodyfikowana w następujący sposób:

• Zamawiający modyfikuje załącznik nr 10 do SWZ – opis przedmiotu zamówienia poprzez:

Wydział Organizacyjny

ul. Zwycięstwa 21
44-100 Gliwice
tel. +48 32 238-55-30
za@um.gliwice.pl

a) wykreślenie w rozdziale III. Zakres ilościowy zamówienia w Lp. 1 (kolumna: przedmiot) zwrotu: "DLP".

powinno być:

"1 Podstawowe moduły zabezpieczające poczty (brama / agent MTA, antyspam, antywirus, kwarantanna, routing, DMARC) — wdrożenie lokalne (on-premise) — użytkownik klasyczny (pełna ochrona).";

b) wykreślenie w rozdziale IV. Wymagania ogólne dotyczące realizacji zamówienia w pkt. 7 zwrotu: "DLP".

powinno być:

"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.";

c) wykreślenie w rozdziale V. Wymagania funkcjonalne i techniczne (wymagania minimalne) pkt. 1 Wdrażanie i zarządzanie, Lp. 5 w brzmieniu:

"5 Rozwiązanie musi zapewniać wdrożenie i stałe monitorowanie DMARC oraz umożliwiać świadczenie usług powiązanych, takich jak archiwizacja wiadomości e-mail i usługi ciągłości działania.";

d) wykreślenie w rozdziale V. Wymagania funkcjonalne i techniczne (wymagania minimalne) pkt. 2 Ochrona przed przejęciem biznesowej poczty e-mail (BEC), Lp. 25 w brzmieniu:

"25 Rozwiązanie musi skutecznie blokować ataki realizowane za pośrednictwem poczty e-mail, w tym Business Email Compromise (BEC), złośliwe oprogramowanie, phishing oraz przejęcie konta poczty e-mail (EAC).";

e) wykreślenie w rozdziale V. Wymagania funkcjonalne i techniczne (wymagania minimalne) pkt. 8 Zapobieganie utracie danych (DLP), Lp. 161-164 w brzmieniu:

"161 Rozwiązanie musi zawierać funkcje zapobiegania utracie danych (DLP)

w wiadomościach e-mail, aby przeciwdziałać nieautoryzowanemu przesyłaniu danych poufnych lub danych osobowych (PII), z możliwością blokowania lub zgłaszania takich transmisji.

162 Rozwiązanie musi obsługiwać bezpieczne opcje szyfrowania wiadomości, w tym TLS oraz szyfrowanie push/pull, w celu ochrony poufnych informacji podczas przesyłania.

163 Rozwiązanie musi umożliwiać bezpieczne wysyłanie dużych plików za pośrednictwem portalu zintegrowanego z rozwiązaniem do szyfrowania poczty.

164 Rozwiązanie musi zapewniać powiadomienia i alerty w czasie rzeczywistym dotyczące naruszeń zasad lub podejrzanych działań związanych z DLP.";

f) zmiana brzmienia w rozdziale V. Wymagania funkcjonalne i techniczne (wymagania minimalne) pkt. 5 Pulpity nawigacyjne oraz raporty o zagrożeniach i użytkownikach, Lp. 89 (po modyfikacji będzie to Lp. 87):

jest:

"Wykonawca powinien dysponować centrum analizy zagrożeń lub łączyć się z nim w celu zapewnienia branżowego testu porównawczego oraz automatycznej aktualizacji i wzbogacania alertów.".

powinno być:

"**Producent** powinien dysponować centrum analizy zagrożeń lub łączyć się z nim w celu zapewnienia branżowego testu porównawczego oraz automatycznej aktualizacji i wzbogacania alertów.";

g) wykreślenie w rozdziale VI. Wdrożenie w tiret trzecie zwrotu: "DLP".

powinno być:

"• konfiguracji modułów zabezpieczających oraz polityk bezpieczeństwa dla poczty przychodzącej i wychodzącej (antyspam, antywirus, antyphishing, ochrona przed BEC, kwarantanna, routing);";

h) dodanie po rozdziale X. Wymagania dotyczące producenta rozwiązania i bezpieczeństwa danych - uwagi o treści:

"UWAGA:

Wszędzie gdzie w OPZ Zamawiający posługuje się sformułowaniami takimi jak „możliwość”, „możliwość rozbudowy”, „możliwość rozszerzenia” lub równoważnymi, Zamawiający nie wymaga dostarczenia odpowiednich dodatkowych licencji w ramach niniejszego zamówienia, lecz wymaga, aby oferowana platforma technicznie umożliwiała uruchomienie wskazanej funkcjonalności poprzez późniejsze rozszerzenie zakresu licencjonowania.".

• Zamawiający modyfikuje załącznik nr 11 do SWZ – formularz zgoności poprzez:

a) wykreślenie w rozdziale Część A. Wymagania ogólne (Sekcja IV OPZ) w Lp. 7 zwrotu: "DLP".

powinno być:

"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.";

b) wykreślenie w rozdziale Część B. Wymagania minimalne (obligatoryjne) pkt. 1 Wdrażanie i zarządzanie, Lp. 5 w brzmieniu:

"5 Rozwiązanie musi zapewniać wdrożenie i stałe monitorowanie DMARC oraz umożliwiać świadczenie usług powiązanych, takich jak archiwizacja wiadomości e-mail i usługi ciągłości działania.";

c) wykreślenie w rozdziale Część B. Wymagania minimalne (obligatoryjne) pkt. 2 Ochrona przed przejęciem biznesowej poczty e-mail (BEC), Lp. 25 w brzmieniu: "25 Rozwiązanie musi skutecznie blokować ataki realizowane za pośrednictwem poczty e-mail, w tym Business Email Compromise (BEC), złośliwe oprogramowanie, phishing oraz przejęcie konta poczty e-mail (EAC).";

d) wykreślenie w rozdziale Część B. Wymagania minimalne (obligatoryjne) pkt. 8 Zapobieganie utracie danych (DLP), Lp. 161-164 w brzmieniu:

"161 Rozwiązanie musi zawierać funkcje zapobiegania utracie danych (DLP) w wiadomościach e-mail, aby przeciwdziałać nieautoryzowanemu przesyłaniu danych poufnych lub danych osobowych (PII), z możliwością blokowania lub zgłaszania takich transmisji.

162 Rozwiązanie musi obsługiwać bezpieczne opcje szyfrowania wiadomości, w tym TLS oraz szyfrowanie push/pull, w celu ochrony poufnych informacji podczas przesyłania.

163 Rozwiązanie musi umożliwiać bezpieczne wysyłanie dużych plików za pośrednictwem portalu zintegrowanego z rozwiązaniem do szyfrowania poczty.

164 Rozwiązanie musi zapewniać powiadomienia i alerty w czasie rzeczywistym dotyczące naruszeń zasad lub podejrzanych działań związanych z DLP.";

e) zmiana brzmienia w rozdziale Część B. Wymagania minimalne (obligatoryjne) pkt. 5 Pulpity nawigacyjne oraz raporty o zagrożeniach i użytkownikach, Lp. 89 (po modyfikacji będzie to Lp. 87):

jest:

"Wykonawca powinien dysponować centrum analizy zagrożeń lub łączyć się z nim w celu zapewnienia branżowego testu porównawczego oraz automatycznej aktualizacji i wzbogacania alertów.".

powinno być:

"**Producent** powinien dysponować centrum analizy zagrożeń lub łączyć się z nim w celu zapewnienia branżowego testu porównawczego oraz automatycznej aktualizacji i wzbogacania alertów.".

Zamawiający informuję, iż w konsekwencji powyższej modyfikacji dokonał również zmiany numeracji "Lp" w załączniku nr 10 i załączniku nr 11 do SWZ - po modyfikacji. Dokumenty otrzymują brzmienie jak załączniki do niniejszego zawiadomienia o modyfikacji specyfikacji warunków zamówienia.

Załączniki:

- 1) załącznik nr 10 do SWZ - opis przedmiotu zamówienia - po modyfikacji,
- 2) załącznik nr 11 do SWZ - formularz zgodności - po modyfikacji.

Na podstawie art. 286 ust. 3 ustawy Prawo zamówień publicznych zamawiający przedłuża termin składania ofert do dnia 24-08-2026 r. do godz. 09:00.

Otwarcie ofert odbędzie się w dniu 24-08-2026 r. o godz. 10:00.

Wykonawca jest związany ofertą do dnia 22-09-2026 r.

Z poważaniem

Monika Szczuk

Kierownik Referatu Zamówień Publicznych