Załącznik do Zapytania o wycenę szacunkową

Szczegółowy opis przedmiotu zamówienia

1. Przedmiot zamówienia:

1) w ramach zamówienia podstawowego:
   a) dostawa subskrypcji oprogramowania Microsoft Enterprise Mobility + Security E3 (EMS E3) lub oprogramowania równoważnego dla 750 użytkowników, na okres 12 miesięcy z terminem obowiązywania od dnia 02.11.2026 r. (dalej jako: „Oprogramowanie");
   b) świadczenie przez Wykonawcę Usługi Wsparcia Technicznego;
2) w ramach zamówienia opcjonalnego, dostawa subskrypcji Oprogramowania obowiązujących przez okres 1 (jednego) miesiąca. Dostawa subskrypcji realizowana będzie w każdym miesiącu w okresie do 12 (dwunastu) miesięcy od dnia 02.11.2026 r., w wymiarze do maksymalnie 100 (stu) sztuk miesięcznie, minimum 10 (dziesięć) sztuk subskrypcji miesięcznie. Prawo opcji zlecane będzie w miarę potrzeb Zamawiającego zgłaszanych w okresie obowiązywania umowy.

Celem zamówienia jest zwiększenie bezpieczeństwa funkcjonowania posiadanej przez Zamawiającego usługi Microsoft Office 365 E5 oraz urządzeń końcowych Zamawiającego.

2. Wymagania ogólne:

1) Oprogramowanie musi pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia;
2) Wykonawca zapewni Zamawiającemu dostęp do portalu producenta w celu dostępu oraz zarządzania licencjami;
3) gwarancja dostępności najnowszej wersji Oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy;
4) możliwość wykorzystania wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego;
5) Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.

3. Usługa Wsparcia Technicznego

Wykonawca zapewni świadczenie usługi wsparcia technicznego i konsultacji dla zaproponowanego rozwiązania, która będzie realizowana przez co najmniej jednego certyfikowanego specjalistę posiadającego certyfikaty na poziomie:

1) Microsoft 365 Certified: Enterprise Administrator Expert;
2) Microsoft Certified: Identity and Access Administrator Associate;
3) Microsoft Certified: Endpoint Administrator Associate

lub równoważne certyfikaty dla zaproponowanego rozwiązania.

Przez certyfikaty równoważne Zamawiający rozumie aktualne certyfikaty producenta oferowanego rozwiązania lub inne dokumenty wystawione przez uprawniony podmiot, potwierdzające posiadanie przez specjalistę wiedzy i umiejętności w zakresie nie mniejszym niż wymagany dla wdrożenia, konfiguracji, administracji, utrzymania oraz świadczenia wsparcia technicznego dla oferowanego rozwiązania, w zakresie obejmującym co najmniej obszary zarządzania tożsamością i dostępem, zarządzania urządzeniami końcowymi oraz bezpieczeństwa i zgodności.

Usługa wsparcia technicznego będzie świadczona w okresie 12 miesięcy od dnia uruchomienia subskrypcji Oprogramowania, w wymiarze nie przekraczającym 120 godzin. Usługa wsparcia obejmuje w szczególności:

1) udzielanie konsultacji i wsparcia technicznego;
2) świadczenie pomocy zdalnej administratorom Zamawiającego.

4. Wymagania dla oprogramowania równoważnego

Opis kryteriów równoważności dla oprogramowania Microsoft Enterprise Mobility + Security E3 stanowi Załącznik nr 1 do SOPZ.

Załącznik nr 1 do SOPZ

Opis wymagań dla oprogramowania równoważnego

1. W przypadku zaoferowania równoważnego produktu, musi on zostać w pełni zintegrowany z obecnie użytkowanymi usługami Microsoft Office 365 E5 oraz aplikacjami Microsoft 365 i musi:
   1) Zawierać centralny katalog tożsamości użytkowników i grup.
   2) Umożliwiać zarządzanie użytkownikami lokalnymi i chmurowymi.
   3) Pozwalać na synchronizację tożsamości z lokalnego Active Directory.
   4) Umożliwiać obsługę środowiska hybrydowego (on-premises + cloud).
   5) Pozwalać na zarządzanie rolami administracyjnymi opartymi na RBAC.
   6) Umożliwiać delegowanie administracji do wybranych ról.
   7) Umożliwiać ograniczanie uprawnień administratorów zgodnie z zasadą least privilege.
   8) Umożliwiać zarządzanie grupami zabezpieczeń.
   9) Umożliwiać zarządzanie grupami Microsoft 365.
   10) Umożliwiać tworzenie dynamicznych grup użytkowników opartych o atrybuty.
   11) Umożliwiać zarządzanie dynamicznymi grupami urządzeń.
   12) Umożliwiać automatyczne aktualizowanie członkostwa grup.
   13) Umożliwiać przypisywanie aplikacji do grup.
   14) Umożliwiać przypisywanie licencji na podstawie grup.
   15) Umożliwiać Single Sign-On (SSO) do aplikacji SaaS.
   16) Umożliwiać SSO do aplikacji on-premises.
   17) Umożliwiać obsługę protokołów SAML 2.0.
   18) Umożliwiać obsługę OAuth 2.0.
   19) Umożliwiać obsługę OpenID Connect.
   20) Umożliwiać integrację z aplikacjami firm trzecich.
   21) Umożliwiać zarządzanie dostępem do aplikacji.
   22) Umożliwiać kontrolę, które grupy użytkowników mają dostęp do aplikacji.
   23) Umożliwiać rejestrowanie logowań użytkowników.
   24) Umożliwiać rejestrowanie adresów IP i lokalizacji logowania.
   25) Umożliwiać rejestrowanie użytych metod uwierzytelnienia.
   26) Pozwalać na logowanie aktywności użytkowników.
   27) Umożliwiać logi audytu zmian w katalogu.
   28) Pozwalać na eksport logów do CSV.
   29) Umożliwiać integrację logów z Azure Monitor.
   30) Umożliwiać integrację z systemami SIEM.
   31) Umożliwiać definiowanie polityk dostępu warunkowego.
   32) Umożliwiać wymuszanie MFA na podstawie warunków.

33) Umożliwiać warunkowanie dostępu na podstawie lokalizacji.
34) Umożliwiać warunkowanie dostępu na podstawie stanu urządzenia.
35) Umożliwiać warunkowanie dostępu na podstawie aplikacji.
36) Umożliwiać wykluczanie zaufanych lokalizacji.
37) Umożliwiać tworzenie oddzielnych polityk dla administratorów.
38) Umożliwiać tworzenie oddzielnych polityk dla użytkowników zewnętrznych.
39) Umożliwiać blokowanie dostępu z urządzeń niezgodnych.
40) Pozwalać na zapraszanie użytkowników zewnętrznych (goście).
41) Umożliwiać dostęp B2B do aplikacji organizacji.
42) Umożliwiać zarządzanie cyklem życia użytkowników gościnnych.
43) Umożliwiać stosowanie dostępu warunkowego dla B2B.
44) Umożliwiać audyt logowań użytkowników zewnętrznych.
45) Umożliwiać ograniczanie uprawnień gości.
46) Pozwalać na blokady konta gościa.
47) Pozwalać na centralną kontrolę dostępu partnerów i kontraktorów.
48) Umożliwiać wieloskładnikowe uwierzytelnianie (MFA).
49) Umożliwiać uwierzytelnianie MFA oparte o aplikację Microsoft Authenticator.
50) Umożliwiać uwierzytelnianie MFA z użyciem SMS i połączeń głosowych.
51) Umożliwiać uwierzytelnianie MFA z użyciem powiadomień push.
52) Umożliwiać uwierzytelnianie MFA dla administratorów.
53) Umożliwiać uwierzytelnianie MFA wymuszane przez Conditional Access.
54) Pozwalać na rejestrowanie prób MFA.
55) Pozwalać na raporty wykorzystania MFA.
56) Umożliwiać zabezpieczenie kont użytkowników bez haseł prostych.
57) Umożliwiać samodzielne resetowanie hasła przez użytkownika.
58) Umożliwiać na MFA jako element potwierdzenia tożsamości przy resecie.
59) Umożliwiać synchronizację resetu hasła z lokalnym Active Directory.
60) Umożliwiać reset hasła z poziomu przeglądarki.
61) Umożliwiać reset hasła z urządzeń mobilnych.
62) Pozwalać na definiowanie metod weryfikacji użytkownika.
63) Pozwalać na logowanie operacji resetu hasła.
64) Pozwalać na raporty dotyczące resetów haseł.
65) Umożliwiać centralne zarządzanie urządzeniami mobilnymi.
66) Umożliwiać zarządzanie urządzeniami z Windows.
67) Umożliwiać zarządzanie urządzeniami z macOS.
68) Umożliwiać zarządzanie urządzeniami z iOS.
69) Umożliwiać zarządzanie urządzeniami z Android.

70) Pozwalać na rejestrację urządzeń w MDM.
71) Umożliwiać automatyczną konfigurację urządzeń (Zero Touch).
72) Umożliwiać wymuszanie polityk bezpieczeństwa urządzeń.
73) Pozwalać na polityki haseł i blokady ekranu.
74) Umożliwiać wymuszanie szyfrowania dysku (BitLocker/FileVault).
75) Pozwalać na sprawdzanie zgodności urządzeń (compliance).
76) Pozwalać na definiowanie reguł zgodności urządzeń.
77) Umożliwiać blokowanie dostępu dla urządzeń niezgodnych.
78) Umożliwiać integrację compliance z Conditional Access.
79) Umożliwiać zdalne usuwanie danych firmowych (wipe).
80) Pozwalać na Selective wipe na urządzeniach prywatnych.
81) Umożliwiać zarządzanie aktualizacjami systemów operacyjnych.
82) Umożliwiać zdalną konfigurację urządzeń bez fizycznego dostępu.
83) Umożliwiać zarządzanie certyfikatami urządzeń.
84) Pozwalać na generowanie raportów stanu urządzeń.
85) Umożliwiać zarządzanie aplikacjami firmowymi.
86) Umożliwiać zdalną instalację aplikacji.
87) Umożliwiać dystrybucję aplikacji ze sklepów publicznych.
88) Umożliwiać White-listing aplikacji.
89) Umożliwiać Black-listing aplikacji.
90) Umożliwiać ochronę danych aplikacji firmowych.
91) Umożliwiać separację danych służbowych i prywatnych.
92) Umożliwiać wymuszanie polityk dostępu do danych aplikacji.
93) Umożliwiać blokowanie kopiowania danych firmowych.
94) Umożliwiać kontrole dostępu do danych aplikacji mobilnych.
95) Umożliwiać widoczność aplikacji SaaS używanych w organizacji.
96) Umożliwiać identyfikację aplikacji typu Shadow IT.
97) Umożliwiać klasyfikację aplikacji według poziomu ryzyka.
98) Pozwalać na monitorowanie aktywności użytkowników w aplikacjach SaaS.
99) Pozwalać na wykrywanie podejrzanych zachowań użytkowników.
100) Umożliwiać rejestrowanie operacji na plikach chmurowych.
101) Pozwalać na alerty o nietypowej aktywności.
102) Umożliwiać integrację z Entra ID.
103) Umożliwiać integrację z Intune.
104) Pozwalać na raportowanie aktywności aplikacji cloud.
105) Umożliwiać ręczną klasyfikację danych.
106) Umożliwiać etykietowanie dokumentów i plików.

107) Umożliwiać etykietowanie danych w Office 365.
108) Umożliwiać ochronę dokumentów przed nieautoryzowanym dostępem.
109) Pozwalać na możliwość ograniczenia edycji dokumentów.
110) Pozwalać na możliwość ograniczenia drukowania dokumentów.
111) Umożliwiać ochronę dokumentów e-mail.
112) Umożliwiać trwałe szyfrowanie plików.
113) Umożliwiać ochronę danych po opuszczeniu organizacji.
114) Pozwalać na podstawowe raporty użycia etykiet.
115) Umożliwiać audyt działań administracyjnych.
116) Umożliwiać audyt zmian konfiguracji zabezpieczeń.
117) Pozwalać na raporty dostępu do aplikacji.
118) Umożliwiać raporty logowań użytkowników.
119) Umożliwiać raporty zgodności urządzeń.
120) Umożliwiać integrację raportów ze SIEM.
121) Umożliwiać wsparcie audytów bezpieczeństwa.
122) Umożliwiać wsparcie zgodności z GDPR.
123) Zapewniać centralny punkt raportowania bezpieczeństwa.
124) Udostępniać Web-owy portal administracyjny.
125) Umożliwiać na dostęp przez HTTPS.
126) Umożliwiać na szyfrowanie danych w tranzycie (TLS).
127) Umożliwiać na szyfrowanie danych w spoczynku.
128) Pozwalać na role oparte o RBAC.
129) Umożliwiać interfejs w języku polskim i angielskim.
130) Umożliwiać wysoką dostępność usługi.
131) Pozwalać na skalowalność dla dużych organizacji.
132) Umożliwiać integrację przez API (Microsoft Graph).
133) Umożliwiać automatyzację procesów IAM.
134) Umożliwiać centralne zarządzanie bezpieczeństwem mobilnym.
135) Zapewniać zgodność z przepisami RODO, a w szczególności art. 28 RODO.
136) Zapewniać zgodność z przepisami art. 23–29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 (Data Act).
137) Zapewnić, iż w okresie obowiązywania subskrypcji, a także po jej zakończeniu, dostawca usług chmurowych (Producent) umożliwi Zamawiającemu bezproblemowe przeniesienie jego danych i zasobów cyfrowych do innego dostawcy lub do infrastruktury własnej Zamawiającego.
138) Zagwarantować, iż z tytułu zmiany dostawcy nie zostaną naliczone żadne opłaty za transfer danych ani inne opłaty o charakterze sankcyjnym.

139) Zapewnić, iż dostarczone i wdrożone narzędzia zapewniają spełnienie wymogów ochrony danych w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default) zgodnie z art. 25 RODO.

2. Usługa Wdrożeniowa

Wykonawca zobowiązuje się wdrożyć Oprogramowanie w środowisku Zamawiającego, w terminie do 15 dni roboczych od dnia zawarcia umowy. Usługa wdrożeniowa obejmuje:

1) przedstawienie harmonogramu prac;
2) migrację/odtworzenie obecnej konfiguracji Zamawiającego;
3) konfigurację umożliwiającą podłączenie/rejestrację urządzeń typu Android, iOS, Windows;
4) konfigurację oraz przygotowanie polityk dla systemów typu Android, iOS, Windows;
5) opracowanie i przekazanie dokumentacji powdrożeniowej (w języku polskim) zawierającej polityki i ich konfigurację oraz czynności jakie zostały wykonane krok po kroku wraz z ich dokładnym opisem.

Prace będą prowadzone z udziałem przedstawicieli Zamawiającego poprzez zdalne połączenie lub obecność w siedzibie Zamawiającego.

3. Usługa Szkoleniowa

Wykonawca zapewni przeprowadzenie szkoleń dla 8 administratorów Zamawiającego obejmujących kompleksowe szkolenie z administrowania zaproponowanym oprogramowaniem w minimalnym wymiarze 5x8 godzin (przez 1 godzinę szkoleniową rozumie się 60 minut), przeprowadzone przez certyfikowanych inżynierów producenta oprogramowania.

Szkolenie odbędzie się w terminie ustalonym przez strony, nie później niż w terminie 3 miesięcy od dnia odbioru Oprogramowania. Szkolenie będzie przeprowadzone stacjonarnie w siedzibie Zamawiającego w Warszawie lub w formie zdalnej. Zamawiający dopuszcza vouchery umożliwiające zapisanie się na szkolenia z oferowanego oprogramowania;