Agencja Oceny Technologii Medycznych
i Taryfikacji

ul. Przeskok 2, 00-032 Warszawa
tel./22/ 101-46-00 fax./22/ 46-88-555
strona internetowa:
www.aotmit.gov.pl
www.bipold.aotm.gov.pl

NIP 525-23-47-183

ZAPYTANIE O CENĘ

Przedmiot ZAPYTANIA - wycena:

Usługi optymalizacji oraz wsparcia technicznego dla środowiska Microsoft 365

I. Przedmiot niniejszego zapytania

Agencja Oceny Technologii Medycznych i Taryfikacji zamierza ogłosić postępowanie mające na celu wyłonienie Wykonawcy, który będzie świadczył usługi optymalizacji oraz wsparcia technicznego dla środowiska Microsoft 365.

Celem niniejszego zapytania jest ustalenie szacunkowej wartości zamówienia, przed ogłoszeniem postępowania o udzielenie zamówienia publicznego – planowanego na grudzień 2024 r.

II. Opis przedmiotu zamówienia dla potrzeb wyceny

Agencja Oceny Technologii Medycznych i Taryfikacji korzysta z rozwiązania Microsoft 365 w subskrypcji Business Premium oraz E3. Obecnie poszukujemy firmy, która w okresie Styczeń-Czerwiec 2025 kompleksowo przeprowadziłaby przegląd obecnej konfiguracji środowiska Microsoft 365 (Azure AD, Exchange Online, obszarów compliance i security itd.). Następnie zostałby sporządzony raport obecnej konfiguracji oraz zaproponowane zostałyby rozwiązania wraz harmonogramem prac konfiguracji dotyczący usług Microsoft 365.

Poniżej został zamieszczony zakres prac, uwzględniający główne założenia jakie firma AOTMiT chciałaby wprowadzić i skonfigurować oraz wymagania wobec Wykonawcy.

Zakres:

1. **Usługa optymalizacji, wsparcia technicznego i konsultacji dla zabezpieczeń środowiska Microsoft 365.**

Usługa dostarcza wsparcia dla platformy Microsoft 365 w trzech obszarach kompetencyjnych:

- Zbadanie i rekomendacja optymalizacji dla obecnego stanu zabezpieczeń platformy
- Wsparcie techniczne w realizacji zadań wymagających wiedzy eksperckiej
- Konsultacje dla wdrażania innowacji wspierających efektywność lub ograniczających ryzyko naruszenia bezpieczeństwa organizacji

Optymalizacja polega na wykonaniu badania stanu aktywnego wykorzystania technologii zabezpieczeń dostępnych w ramach subskrypcji Microsoft 365 Business Premium / E3 / Defender for Business / Endpoint P2.
Zakres badania powinien obejmować obszary Microsoft 365:

- Konfiguracja brzegowych zabezpieczeń usługi Microsoft Entra ID
- Tożsamość i dostęp
- Zarządzanie zabezpieczeniami poczty
- Zarządzanie urządzeniami
- Zarządzanie zabezpieczeniami punktów końcowych
- Zarządzanie aplikacjami
- Bezpieczeństwo informacji
- Zarządzanie cyklem życia informacji
- Zarządzanie aktualizacjami

Badanie powinno skwantyfikować skalę użycia środków zabezpieczeń technicznych (np. przez % użytkowników objętych zasadami zabezpieczeń, % aktywnie korzystających z funkcjonalności zabezpieczeń – tam, gdzie to możliwe) lub skalę stosowania ochrony przynajmniej dla następujących kategorii:

- Konfiguracja dostępu awaryjnego

- Dostosowanie strony logowania do usług Microsoft 365
- Włączenie zasad dot. metod uwierzytelniania
- Samoobsługowe resetowanie hasła
- Użycie metod logowania bez użycia hasła (Passkey, FIDO2)
- Współpraca z kontami z innych środowisk chmurowych platformy Microsoft 365, B2B, Cross-Tenant
- Synchronizacja usługi Active Directory z Entra ID
- Synchronizacja skrót haseł usługi Active Directory użytkownika z Entra ID
- Zapisywanie zwrotne haseł na potrzeby samoobsługowego resetowania haseł
- Rejestracja urządzeń w Entra ID (device registration)
- Przyłączanie urządzeń do Entra ID (Entra hybrid / join)
- Rejestracja urządzeń w zarządzaniu Intune MDM (Intune enrollment)
- Uwierzytelnienie dla poczty za pomocą kluczy domeny (DKIM)
- Stosowanie DMARC (Domain-based Message Authentication, Reporting, and Conformance)
- Stosowanie zasad ochrony dla poczty e-mail i współpraca z zasadami usługi Defender Office 365
- Stosowanie zasad ochrony przed spamem i phishingiem
- Zapobieganie utracie danych (Exchange, SharePoint, OneDrive, Teams)
- Stosowanie klasyfikacji informacji
- Stosowanie ochrona informacji przez szyfrowanie dokumentów i wiadomości
- Manulane lub domyślne etykietowanie poufności w aplikacjach Microsoft 365
- Szyfrowanie wiadomości technologią Defender for Office 365
- Zasady przechowywania w organizacji lub lokalizacji lub usłudze (retention policies)
- Przechowywanie wiadomości w usłudze Teams i SharePoint dla Grup Microsoft 365 (retention policies)
- Włączenie Audit Log
- Konfiguracja ograniczeń dla rejestracji urządzeń wg obsługiwanych platform
- Zasady zgodności dla urządzeń
- Zasady szyfrowania urządzeń
- Ochrona danych w aplikacjach mobilnych Intune App Protection Policies
- Zasady dostępu z urządzeń prywatnych
- Zarządzanie pakietem Microsoft 365
- Zarządzanie aktualizacjami
- Zarządzanie podatnościami
- Zasady dotyczące instalacja aplikacji
- Instalowanie i konfigurowanie usługi Microsoft Defender dla Firm / Endpoint P2
- Konfiguracja zasad usługi Defender Defender dla Firm / Endpoint P2

Z badania powinny wynikać:

- Skala użycia
- Rekomendacje optymalizacji
- Rekomendacje do zmiany / zwiększenia skali wykorzystania

Dodatkowym celem badania jest uzyskanie wiedzy niezbędnej do samooceny organizacji w kontekście zgodności zabezpieczeń platformy Microsoft 365 z dyrektywą NIS2.
Link do dyrektywy:
https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022L2555#d1e3362-80-1

2. Wsparcie: Utrzymanie infrastruktury Microsoft 365 jako wsparcie eksperckie Level 3 w wymiarze do 20 roboczogodzin w miesiącu w okresie Styczeń-Grudzień 2025.

Technologie Microsoft podlegające wsparciu:

- Azure Active Directory Premium P1/P2
- Azure Information Protection Premium P1
- Azure Rights Management
- App Protection Policies
- Data Loss Prevention
- Defender for Office 365 (plan 1)
- Exchange Online (Plan 1/2)
- Exchange Online Archiving
- Microsoft 365 Apps for Business / Enterprise
- Microsoft Azure Multi-Factor Authentication
- Microsoft Defender for Cloud Apps Discovery
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Business / for Endpoint P2
- Microsoft Intune Plan 1
- Personal Data Protection for Windows 11
- SharePoint (Plan 1)
- Windows Autopilot v1/v2 (Device Preparation Policies)
- Windows 10/11 Business / Enterprise
- Windows Mobile App Management
- Windows Update for Business Deployment Service

3. Wymagania dla dostawcy

- Aktywny status dostawcy w programie akredytacyjnym Microsoft - Microsoft Solutions Partner Modern Work
- Aktywny Certyfikat pracownika wykonującego zadania optymalizacji, wsparcia i konsultacji dla innowacji: Microsoft 365 Certified Administrator Expert.
- Przygotowanie komunikacji wewnętrznej (użytkownicy) dla zmian wpływających na użytkowników i ich korzystanie z usługi Microsoft 365 / urządzeń
- Przeprowadzenie szkolenia administratorów z ww. zakresu prac
- Przygotowanie i aktualizacja dokumentacji wdrożeniowej
- Przygotowanie komunikacji wewnętrznej (użytkownicy) dla zmian wpływających na użytkowników i ich korzystanie z usługi Microsoft 365 / urządzeń

III. Termin przesłania wyceny

Ostateczny termin wyceny**: do dnia 13.12.2024 r. do godz. 17:00**

IV. Zwrot kosztów udziału w postępowaniu

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

V. Sposób przekazania wyceny.

1. Wycenę należy wysłać na adres e-mail: zp@aotm.gov.pl

VI. Opis sposobu przygotowania wyceny

W oparciu o przedłożone dokumenty proszę o podanie ceny **brutto i netto, za wykonanie przedmiotowego zamówienia.**
Cena ma uwzględniać wszystkie koszty (dot. składników przedmiotu zamówienia określone w OPZ).