

ZAŁĄCZNIK NR 1

OPIS PLANOWANEGO ZAKRESU USŁUGI ORAZ PODSTAWOWE INFORMACJE DO PRZYGOTOWANIA WYCENY

Usługa diagnostyczno-analityczna w zakresie dostosowania Urzędu do wymagań KSC/NIS2

1. Cel planowanej usługi

Urząd Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 planuje realizację pierwszego etapu prac związanych z dostosowaniem Urzędu do wymagań KSC/NIS2.

Celem usługi będzie ocena stanu obecnego (gap analysis) jako punkt wyjścia do dalszych decyzji, identyfikacja luk i ryzyk oraz przygotowanie podstaw do zaplanowania dalszych działań dostosowawczych.

Usługa będzie miała charakter diagnostyczno-analityczny. Nie stanowi audytu, o którym mowa w art. 15 ustawy o krajowym systemie cyberbezpieczeństwa, ani kompleksowego wdrożenia systemu zarządzania bezpieczeństwem informacji.

2. Planowany zakres

1. Weryfikacja obowiązków KSC/NIS2 dotyczących Urzędu oraz ocena aktualnego stanu - w tym posiadanej dokumentacji, procesów, systemów oraz stosowanych zabezpieczeń organizacyjnych i technicznych.

2. Identyfikacja kluczowych zasobów, ich właścicieli i zależności - w tym istotnych zależności od dostawców i usług zewnętrznych, oraz ocena potrzeb w zakresie ciągłości działania.

3. Analiza luk i ryzyka - przeprowadzona na podstawie zweryfikowanych informacji i dowodów, obejmująca ocenę istniejących zabezpieczeń oraz wskazanie najistotniejszych ryzyk i obszarów wymagających działań.

4. Przygotowanie rekomendacji i planu dalszych działań - ze wskazaniem priorytetów i proponowanej kolejności realizacji, orientacyjnego harmonogramu, orientacyjnych kosztów, zadań możliwych do wykonania zasobami własnymi Urzędu oraz zadań wymagających specjalistycznego wsparcia zewnętrznego.

5. Przygotowanie neutralnych technologicznie wymagań merytorycznych, organizacyjnych i technicznych - wynikających ze zidentyfikowanych potrzeb, które będą mogły zostać wykorzystane przez Urząd jako materiał źródłowy przy przygotowywaniu ewentualnych przyszłych zamówień.

Materiał dotyczący wymagań dla dalszych działań będzie miał charakter rekomendacyjny i źródłowy i nie będzie stanowił opisu przedmiotu zamówienia dla przyszłego postępowania.

3. Zakładane rezultaty

- raport z przeprowadzonych prac;
- macierz zgodności;
- rejestr zidentyfikowanych luk i ryzyk;
- plan dalszych działań powiązany z ustaleniami i dowodami;
- neutralne technologicznie wymagania dla dalszych działań;
- prezentacja wyników kierownictwu Urzędu.

Dokumenty powinny zostać przekazane w formie elektronicznej, w tym w formatach umożliwiającym ich dalszą edycję i wykorzystanie przez Urząd.

4. Podstawowe informacje o organizacji

Urząd jest urzędem państwowym działającym w jednej lokalizacji w Polsce.

Łączna liczba pracowników i współpracowników wynosi około 65-70 osób. Z systemów IT korzysta 57 osób, wliczając pracowników oraz współpracowników świadczących usługi w modelu B2B.

Urząd należy do sektora publicznego i ze względu na specyfikę działalności przetwarza informacje wymagające odpowiedniego poziomu ochrony.

5. Podstawowe informacje o środowisku IT

Środowisko IT ma charakter hybrydowy i obejmuje infrastrukturę lokalną oraz usługi chmurowe Microsoft 365. Według danych przekazanych na potrzeby rozeznania środowisko obejmuje:

- 149 stacji roboczych;
- 44 serwery wirtualne;
- 3 fizyczne węzły VxRail stanowiące środowisko wirtualizacyjne vSphere;
- serwer kopii zapasowych;
- serwer/repozytorium kopii zapasowych;
- urządzenie Data Domain wykorzystywane do przechowywania kopii zapasowych;
- drugie środowisko wirtualizacyjne obejmujące 3 serwery oraz dodatkową macierz dyskową dla środowiska vSphere;
- 27 aktywnych urządzeń sieciowych.

Do systemów istotnych z perspektywy działalności Urzędu należą w szczególności: Enova, EZD RP, Płatnik, Active Directory oraz Microsoft 365 E5, w tym m.in. OneDrive i SharePoint.

Urząd korzysta z pakietu Microsoft 365 E5 w modelu SaaS. Dla organizacji utrzymywany jest jeden centralny tenant Microsoft 365 obejmujący pracowników i współpracowników B2B.

6. Segmentacja środowiska

W architekturze funkcjonują wyodrębnione sieci i segmenty przeznaczone m.in. dla urządzeń technicznych/OT, sieci zarządzającej, telefonii oraz środowiska wirtualizacji. Separacja pomiędzy poszczególnymi obszarami realizowana jest logicznie z wykorzystaniem sieci VLAN.

7. Informacje istotne dla określenia pracochłonności

Urząd nie posiada obecnie kompletnego, sformalizowanego procesu zarządzania ryzykiem bezpieczeństwa informacji obejmującego metodykę, rejestr ryzyk, kryteria akceptacji i plan postępowania z ryzykiem. Pełna analiza ryzyka nie była dotychczas przeprowadzana.

W okresie ostatnich 24 miesięcy, według informacji przekazanych na potrzeby wcześniejszego rozeznania, nie przeprowadzono pełnych audytów bezpieczeństwa, testów penetracyjnych ani ocen zgodności, których raporty i plany naprawcze mogłyby stanowić podstawę obecnej analizy.

Głównym punktem kontaktowym dla projektu będzie Dyrektor Generalny. Realizacja usługi będzie wymagała współpracy w szczególności z przedstawicielami kierownictwa, IT oraz innych komórek właściwych dla analizowanych obszarów.

Szczegółowe informacje dotyczące architektury, konfiguracji i stosowanych zabezpieczeń nie są udostępniane na etapie rozeznania w zakresie, w jakim nie jest to konieczne do sporządzenia wyceny.

8. Termin realizacji

Zakłada się zawarcie umowy oraz wykonanie, odbiór i rozliczenie całości prac w 2026 r.

Na potrzeby wyceny prosimy o wskazanie minimalnego realnego czasu realizacji usługi oraz najpóźniejszego terminu zawarcia umowy pozwalającego na wykonanie i odbiór prac do końca 2026 r.

9. Dodatkowe informacje potrzebne do wyceny

Jeżeli przedstawione informacje nie są wystarczające do rzetelnego oszacowania ceny, prosimy o wskazanie dodatkowych informacji niezbędnych do przygotowania wyceny.