Załącznik nr 1 do Zapytania ofertowego nr WP.042.4.3.2026.AM

Opis przedmiotu zamówienia

na wykonanie audytu wpływu modernizacji infrastruktury sprzętowej na poprawę cyberbezpieczeństwa dla Starostwa Powiatowego w Szczecinku, Domu Pomocy Społecznej w Bornem Sulinowie i Zespołu Szkół Nr 7 w Białym Borze, w ramach projektu grantowego „Cyberbezpieczny samorząd" Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Przedmiotem zamówienia jest wykonanie audytu w zakresie wpływu modernizacji infrastruktury sprzętowej na poprawę cyberbezpieczeństwa dla trzech jednostek organizacyjnych Powiatu Szczecineckiego:

1. Starostwa Powiatowego w Szczecinku, ul. Warcisława IV 16, 78-400 Szczecinek,
2. Domu Pomocy Społecznej w Bornem Sulinowie, ul. Szpitalna 5, 78-449 Borne Sulinowo,
3. Zespołu Szkół nr 7 w Białym Borze, ul. Brzeźnicka 10, 78-425 Biały Bór.

Celem audytu jest ocena, w jakim stopniu zakup i wdrożenie nowej infrastruktury sprzętowej przyczyniły się do ograniczenia ryzyk cyberbezpieczeństwa oraz zwiększenia odporności infrastruktury IT.

Wykonanie audytu musi uwzględniać diagnozę na dzień rozpoczęcia projektu oraz stan po zakupie i wdrożeniu nowej infrastruktury. Przeprowadzenie audytu musi pozwolić na ocenę, w jakim stopniu zakup i wdrożenie nowej infrastruktury sprzętowej przyczyniły się do ograniczenia ryzyk cyberbezpieczeństwa oraz zwiększenia odporności infrastruktury IT. Audyt ma potwierdzić, czy w wyniku realizacji projektu grantowego podniesiony został poziom cyberbezpieczeństwa i czy osiągnięte zostały cele projektu. W wyniku audytu mają zostać przygotowane raporty podsumowujące zawierające omówienie wszystkich niezgodności.

Zakres audytu obejmuje:

1. Audyt powinien obejmować w szczególności analizę stanu infrastruktury sprzętowej przed przeprowadzoną modernizacją oraz ocenę jej stanu po wdrożeniu zakupionego sprzętu, z uwzględnieniem zmian mających znaczenie dla bezpieczeństwa infrastruktury teleinformatycznej.
2. Głównym założeniem audytu jest określenie, w jakim zakresie wymiana lub rozbudowa infrastruktury sprzętowej:
   a) ograniczyła ryzyka związane z wykorzystaniem przestarzałego lub niewspieranego sprzętu,
   b) zwiększyła odporność infrastruktury na awarie i zakłócenia,

c) poprawiła możliwości stosowania mechanizmów ochrony infrastruktury teleinformatycznej,

d) zwiększyła poziom bezpieczeństwa fizycznego i technicznego urządzeń,

e) wpłynęła na ograniczenie potencjalnej powierzchni ataku,

f) poprawiła możliwości zapewnienia ciągłości działania kluczowych usług i systemów.

3. Audyt powinien uwzględniać w szczególności sprzęt komputerowy, serwerowy, sieciowy, urządzenia bezpieczeństwa sieciowego, urządzenia infrastruktury technicznej oraz nośniki danych – w zakresie objętym modernizacją.
4. Ocena powinna być przeprowadzona w oparciu o porównanie stanu infrastruktury przed modernizacją i po jej przeprowadzeniu, z wykorzystaniem możliwych do zweryfikowania danych, dokumentacji, ewidencji sprzętu oraz oględzin infrastruktury.
5. Wykonawca powinien wskazać najważniejsze zmiany wprowadzone w wyniku modernizacji oraz określić ich wpływ na ograniczenie zidentyfikowanych ryzyk cyberbezpieczeństwa.
6. Wyniki audytu powinny umożliwiać Zamawiającemu wykazanie mierzalnych efektów przeprowadzonej modernizacji, w szczególności poprzez wskazanie różnic pomiędzy stanem przed i po modernizacji oraz określenie poziomu ograniczenia poszczególnych ryzyk.
7. Audyt powinien mieć charakter oceniający i nie powinien ograniczać się wyłącznie do weryfikacji zgodności posiadanego sprzętu z wymaganiami technicznymi. Wykonawca powinien ocenić rzeczywisty wpływ modernizacji na poziom bezpieczeństwa infrastruktury.
8. Zakres audytu powinien koncentrować się na aspektach związanych z infrastrukturą sprzętową. Analiza oprogramowania, aplikacji oraz procesów organizacyjnych powinna zostać uwzględniona wyłącznie w zakresie niezbędnym do oceny wpływu modernizacji sprzętowej na cyberbezpieczeństwo.
9. Zakres audytu musi uwzględniać wymagania proceduralne ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.) dalej nazwane u.o KSC oraz rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773) dalej nazwane KRI.

Dokumentacja po zakończeniu audytów

Po zakończeniu audytu Wykonawca przygotuje raport zawierający wnioski dotyczące stanu obecnego, wytyczne do dalszego doskonalenia i rekomendacje w zakresie poprawy cyberbezpieczeństwa na przyszłość. Raport z audytu zostanie podpisany przez audytora dokonującego audytu. Dokumentacja poaudytowa musi obejmować co najmniej:

- Wprowadzenie (cel audytu, zakres, kluczowe obszary audytowane, datę przeprowadzenia audytu, opis jednostki);
- Opis zastosowanych metod i działań audytowych;

- Ocenę zgodności z przepisami: Ogólna ocena stopnia zgodności odpowiednio z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.), KRI oraz innymi regulacjami i normami, takimi jak RODO lub ISO 27001;
- Identyfikację niezgodności: Wyszczególnienie obszarów, w których audyt wykazał brak zgodności
  z wymaganiami prawnymi lub procedurami wewnętrznymi. Każda niezgodność powinna być opisana i sklasyfikowana (np. krytyczna, wysoka, średnia, niska),
- Wyniki audytu, w tym:
  - wskazanie słabych punktów w zabezpieczeniach technicznych;
  - ocenę ryzyka – analizę wykrytych ryzyk związanych z bezpieczeństwem informacji, obejmującą ryzyka dla integralności, poufności i dostępności danych oraz systemów;
- Rekomendacje i zalecenia audytorów zawierające:
- Podpisy i oświadczenia audytorów (np. o rzetelności przeprowadzonego audytu i pełnym przedstawieniu wyników oraz wniosków);
- Załączniki (np. listę uczestników audytu, listę przeanalizowanych dokumentów, polityk i procedur, listę sprzętu, konfigurację sieci).