

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest wykonanie dla Państwowej Akademii Nauk Stosowanych we Włocławku Warsztat Audytu cyberbezpieczeństwa wraz z audytem zgodności z dyrektywą NIS2.

1.1. Zakres usługi:

Przeprowadzenie audytu cyberbezpieczeństwa zgodnego z CIS CONTROLS w najnowszej obowiązującej wersji oraz wykonanie audytu zgodności z dyrektywą NIS2.

Usługa ma na celu przeprowadzenie kompleksowego audytu cyberbezpieczeństwa zgodnego z metodologią CIS CONTROLS oraz audytu zgodności z Dyrektywą NIS2.

Audyt obejmuje ocenę stanu obecnego, identyfikację ryzyk oraz zaleceń działań naprawczych. Celem jest weryfikacja 18 kluczowych obszarów cyberbezpieczeństwa oraz identyfikacja, w jakich obszarach zamawiający posiada braki w kontekście Dyrektywy NIS2 oraz uzyskanie informacji jakie inwestycje są kluczowe, aby spełnić wymagania.

1.2. Zakres:

Przedmiot zlecenia w siedzibie Zamawiającego i/lub w trybie online. Zamawiający wymaga co najmniej 1 wizyty w siedzibie Zamawiającego.

1.2.1 Dokładna analiza 18 obszarów:

1. inwentaryzacja i kontrola aktywów
2. inwentaryzacja i kontrola oprogramowania
3. ochrona danych
4. bezpieczeństwo konfiguracji
5. zarządzanie kontami (tożsamością)
6. zarządzanie i kontrola dostępu
7. zarządzanie podatnościami
8. zarządzanie logami
9. ochrona poczty elektronicznej i przeglądarek
10. ochrona przed złośliwym kodem
11. odzyskiwanie danych
12. zarządzanie infrastrukturą sieciową
13. monitorowanie i ochrona sieci
14. budowanie świadomości o zagrożeniach
15. zarządzanie dostawcami usług
16. bezpieczeństwo oprogramowania – rozwój
17. zarządzanie incydentami
18. testy penetracyjne

Zlecenie zakończone szczegółowym raportem.

1.2.2 Zgodność z Dyrektywą NIS2.

Ocena w jakim stopniu PANS we Włocławku stosuje się do wymogów Dyrektywy NIS2, szczególnie w zakresie zarządzania ryzykiem, raportowania incydentów i współpracy w zakresie cyberbezpieczeństwa, w tym ocena procedur reagowania na incydenty i zarządzania ryzykiem. Analiza sposobu w jaki PANS we Włocławku reaguje na incydenty bezpieczeństwa oraz zarządza ryzykiem, w kontekście wymogów Dyrektywy NIS2.

Usługa zakończona szczegółowym raportem z przeprowadzonych prac.

1.3. Metodologia Audytu:

Audytorzy podejmą szereg zaplanowanych i systematycznych działań, aby zapewnić pełne zrozumienie systemów, procesów i procedur obowiązujących w PANS we Włocławku. Metodologia audytu będzie obejmowała:

1. Analiza Dokumentacji:

- a. Przegląd i ocena wszystkich istniejących dokumentów polityk bezpieczeństwa, procedur operacyjnych i innych powiązanych z nimi zapisów.
- b. Sprawdzenie zgodności dokumentacji z obowiązującymi przepisami prawnymi, standardami branżowymi i najlepszymi praktykami.
- c. Wywiady z osobami odpowiedzialnymi za zarządzanie bezpieczeństwem informacji, IT oraz przestrzeganie przepisów RODO.

2. Ocena zgodności z prawem i standardami

- a. Sprawdzenie czy praktyki i systemy są zgodne z lokalnymi i międzynarodowymi przepisami, w tym dyrektywy NIS2.
- b. Analiza zgodności z normami ISO i innymi standardami dotyczącymi bezpieczeństwa informacji.

3. Zarządzanie ciągłością działania.

4. Zarządzanie incydentami bezpieczeństwa informacji.

5. Kopie bezpieczeństwa. 6. Analiza ryzyka bezpieczeństwa informacji.

1.4. Dostarczone Wyniki:

- szczegółowy raport audytowy oceny stanu cyberbezpieczeństwa wraz z identyfikacją potencjalnych luk oraz rekomendacjami audytorów.
- szczegółowy raport zgodności z Dyrektywą NIS2 wraz z opracowaniem kolejnych działań mających na celu zapewnienie zgodności.

1.5. Rekomendacje Działań Naprawczych:

- dokumentacja Proponowanych Usprawnień. Dostarczenie szczegółowych opisów i wytycznych dotyczących proponowanych zmian.
- opracowanie propozycji zmian w istniejących procedurach lub opracowanie projektu nowych procedur tam, gdzie to konieczne.

1.6. Wymagania dla Audytorów:

Audytory wykonujący zadanie muszą posiadać doświadczenie w przeprowadzaniu audytów IT, NIS2, posiadanie odpowiednich certyfikatów branżowych oraz znajomość specyfiki sektora finansów publicznych.

1.7. Sposób realizacji:

Audyt cyberbezpieczeństwa oraz audyt zgodności z dyrektywą NIS2 zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym, jednak nie później niż 60 dni od podpisania umowy. Wykonawca udostępni listę kontrolną Zamawiającego w ciągu 14 dni od podpisania umowy. Akceptowalna jest elektroniczna forma dostarczania dokumentacji.

1.8. Wymagania Organizacyjne:

- audytory będą mieli zapewniony dostęp do wszystkich niezbędnych informacji, dokumentów oraz zasobów organizacji.
- organizacja zapewni współpracę pracowników oraz dostęp do lokalizacji objętych audytem.

1.9. Terminy:

Szczegółowy harmonogram audytów zostanie ustalony przez Zamawiającego w porozumieniu z Wykonawcą. Wykonawca przedstawi do akceptacji harmonogram prac w terminie najpóźniej 7 dni od podpisania umowy. Zakres prac musi być zrealizowany przez 60 dni. Odbiór prac na podstawie protokołu zdawczo-odbiorczego wystawionego przez Wykonawcę i zaakceptowanego przez Zamawiającego.

2. Pozostałe informacje:

- audyty zostaną przeprowadzone zgodnie z najlepszymi praktykami i obowiązującymi standardami audytu
- wszystkie działania audytowe muszą być prowadzone z zachowaniem poufności i dbałością o integralność danych oraz procesów organizacji.
- Liczba zatrudnionych pracowników: 179 osób, w tym 53 pracowników administracyjnych i 126 nauczycieli akademickich
- Liczba lokalizacji: 5 budynków, w tym 1 w przebudowie
- Osoby do kontaktu: Robert Kwaśniewski tel.: +48 511 572 179, e-mail: iod@pans.wloclawek.pl (sprawy IODO), Jarosław Struś tel. 698-075-480, jaroslaw.strus@pans.wloclawek.pl (sprawy IT).