Szacowanie wartości zamówienia na:
„Wykonanie dla Państwowej Akademii Nauk Stosowanych we Włocławku Warsztat Audytu cyberbezpieczeństwa wraz z audytem zgodności z dyrektywą NIS2”

Do Zamawiającego wpłynęły pytania dot. poszczególnych punktów Opisu Przedmiotu Zamówienia.
Zamawiający poniżej zamieścił odpowiedzi na przesłane pytania:

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

Pyt. 1: Czy liczba wizyt ma być wskazana przez Oferenta? Czy Zamawiający zastrzega sobie prawo do wymagania dodatkowych wizyt?
Odpowiedź: Zamawiający wymaga co najmniej 1 wizyty w siedzibie Zamawiającego. Ilość wizyt musi być dostosowana do potrzeb powstałych w trakcie trwania umowy i nie wymaga się od Oferenta deklaracji ilości wizyt.

1.2.1 Dokładna analiza 18 obszarów:
1. inwentaryzacja i kontrola aktywów:
Pyt.2. : Czy Oferent ma przeprowadzić inwentaryzację, czy dostarczyć wytyczne do prawidłowej inwentaryzacji?
Odpowiedź: Oferent ma przeprowadzić inwentaryzację.

3. ochrona danych:
Pyt.3 : Czy Zamawiający wymaga audytu RODO?
Odpowiedź: Tak – w ramach umowy Zamawiający wymaga audytu RODO.

4. bezpieczeństwo konfiguracji:
Pyt.4. : Czy Zamawiający wymaga audytu konfiguracji systemów?
Odpowiedź: Nie znając systemów często specyficznych dla uczelni wyższych nie będziecie Państwo w stanie zweryfikować ich konfiguracji. Prosimy jednak o weryfikację umów serwisowych / helpdesk-owych.

15. zarządzanie dostawcami usług
Pyt.5. : Czy Zamawiający wymaga analizy umów z dostawcami, czy audytu polityk?
Odpowiedź: Zamawiający wymaga audytu umów z dostawcami i polityk.

Pkt. od 5 do 18:
Pyt.6. : Czy Zamawiający wymaga audytu technicznego w tym zakresie, czy audytu polityk?
Odpowiedź: Zamawiający wymaga audytu technicznego i polityk

1.3. Metodologia Audytu:
2. Ocena zgodności z prawem i standardami

2a. Sprawdzenie czy praktyki i systemy są zgodne z lokalnymi i międzynarodowymi przepisami, w tym dyrektywy NIS2

Pyt. 7 : Prośba o podanie o jakie przepisy i standardy chodzi?
Odpowiedź: Ustawa o ochronie danych osobowych z 10 maja 2018 roku, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Rozporządzenie 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 i inne o ile są niezbędne.

pyt.8.: Czy Zamawiający wymaga sprawdzenia również zgodności z innymi aktami, poza NIS2? Jeżeli tak to jakimi?
Odpowiedź: Ustawa o ochronie danych osobowych z 10 maja 2018 roku, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Rozporządzenie 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 i inne o ile są niezbędne.

2b. Analiza zgodności z normami ISO i innymi standardami dotyczącymi bezpieczeństwa informacji.
pyt.9. : Czy audyt ma zawierać nie tylko zgodność z NIS 2, ale również z ISO 27001? Czy również ISO 22301? Czy jeszcze innymi?
Odpowiedź: Audyt powinien dotyczyć norm ISO, które dotyczą uczelni publicznych wg dyrektywy NIS 2.

3. Zarządzanie ciągłością działania.
pyt.10. : Co wymagane jest w zakresie ciągłości działania? Czy posiadają Państwo istniejące polityki i systemy Ciągłości działania, czy mają być stworzone od nowa? Proszę o potwierdzenie, że chodzi o ciągłość działania w obszarze systemów IT.
Odpowiedź: Tak chodzi o ciągłość działania w obszarze systemów IT. Nie mamy spisanej polityki ciągłości działania.

1.5. Rekomendacje Działań Naprawczych: opracowanie propozycji zmian w istniejących procedurach lub opracowanie projektu nowych procedur tam, gdzie to konieczne.

pyt.11. : Jakie polityki i procedury istnieją już u Państwa?
Odpowiedź: Polityka bezpieczeństwa informacji; Instrukcja zarządzania systemami informatycznymi; Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony; Procedury bezpieczeństwa eksploatacji systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w

Państwowej Akademii Nauk Stosowanych we Włocławku; Procedury Szczególnych wymagań bezpieczeństwa systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Państwowej Akademii Nauk Stosowanych we Włocławku; Zarządzenie Rektora Nr 28/19 z dnia 25 marca 2019 roku w sprawie wprowadzenia "Metodyki szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Państwowej Wyższej Szkole Zawodowej we Włocławku";

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.

pyt.12. : Co rozumiane jest pod "Lista kontrolna Zamawiającego"?
Odpowiedź: Pod Listą kontrolną rozumie się wykaz dokumentów jakie Zamawiający ma przygotować dla audytorów. W tekście jest omyłka pisarska powinno być “Lista kontrolna dla Zamawiającego”.

1.8. Wymagania Organizacyjne: audytorzy będą mieli zapewniony dostęp do wszystkich niezbędnych informacji, dokumentów oraz zasobów organizacji.

pyt.13. : Czy Zamawiający udostępni dokumenty online?
Odpowiedź: Tak ale wykonawca musi stworzyć bezpieczny kanał dla w/w dokumentów.

2. Pozostałe informacje: Liczba lokalizacji: 5 budynków, w tym 1 w przebudowie.

pyt.14. : Czy wszystkie budynki znajdują się w 1 lokalizacji/ pod jednym adresem ? Czy budynki mają różne funkcje? Jeśli tak to jakie?
Odpowiedź: 3 lokalizacje, 6 budynków. Pozostałe informacje na naszej stronie: https://pans.wloclawek.pl/baza-dydaktyczna/