Załącznik nr 1 do Zapytania

INP.7013.54.2024

Szczegółowy opis przedmiotu zamówienia

1) **ZAMÓWIENIE OBEJMUJE 5 ZADAŃ DO WYKONANIA:**

Zadanie 1:

Wykonanie audytu wstępnego systemu zarządzania bezpieczeństwem informacji (SZBI) w Urzędzie Miejskim w Poniatowej;

Zadanie 2:

Opracowanie nowych polityk i aktualizacja dokumentacji w ramach wdrożenia SZBI w Urzędzie Miejskim w Poniatowej;

Zadanie 3:

Przeprowadzenie szkoleń z zakresu bezpieczeństwa informacji oddzielnie dla kadry zarządzającej Urzędu Miejskiego w Poniatowej oraz dla pozostałych pracowników Urzędu;

Zadanie 4:

Przeprowadzenie szkoleń z zakresu cyberbezpieczństwa dla pracowników Urzędu Miejskiego w Poniatowej;

Zadanie 5:

Wykonanie audytu końcowego systemu zarządzania bezpieczeństwem informacji (SZBI) w Urzędzie Miejskim w Poniatowej;

2) **Jednostki objęte zamówieniem:**
Urząd Miejski w Poniatowej
3) **Liczba osób objętych szkoleniami:**
– 50 pracowników Urzędu Miejskiego w Poniatowej
4) **Ilość stacji roboczych:** 65 szt.
5) **Ilość serwerów:** 3 szt.
6) **Ilość urządzeń sieciowych:** 36 szt.

7) **OPIS PRZEDMIOTU ZAMÓWIENIA dla zadania nr 1:**

1. Szczegółowe wymagania dotyczące audytu wstępnego:
   1.1. Liczba jednostek objętych audytem wstępnym: 1 (Urząd Miejski w Poniatowej)
   1.2. Miejsce przeprowadzenia audytu: Siedziba Urzędu: ul. Młodzieżowa 2, 24-320 Poniatowa.
   1.3. Zakres audytu wstępnego:
   1.3.1 Ocena poziomu bezpieczeństwa organizacyjnego związanego z posiadaną dokumentacją i procedurami.
   1.3.2 Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
   1.3.3 Przeprowadzenie testów penetracyjnych obejmujących testy styku sieci lokalnej z Internetem (Analiza topologii brzegu sieci, Weryfikacja mechanizmów ochronnych, Próba wykrycia usług sieciowych udostępnianych do Internetu, Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet, Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet.

1.3.4 Przeprowadzenie testów penetracyjnych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego (Analiza topologii sieci LAN, Weryfikacja mechanizmów ochronnych w sieci, Analiza komunikacji sieciowej, Skanowanie portów TCP/UDP i próba wykrycia usług sieciowych, Skanowanie hostów aktywnych w sieci, Exploitacja dostępnych urządzeń oraz usług w sieci LAN.

1.4 Zakres przeprowadzonego audytu w oparciu o przepisy i normy:

1.4.1 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.

1.4.2 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

1.4.3 Ustawa o krajowym systemie cyberbezpieczeństwa.

1.4.4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679

1.4.5 Normy ISO 27001.

1.5 Raport z audytu wstępnego musi zawierać informacje o stanie aktualnym, stwierdzonych uchybieniach oraz zalecenia pokontrolne

1.6 Forma przekazania i omówienia raportu: Spotkanie w siedzibie Urzędu, podczas którego wyniki audytu zostaną omówione z kadrą kierowniczą.

8) OPIS PRZEDMIOTU ZAMÓWIENIA dla zadania nr 2

Opracowanie nowych polityk i aktualizacja dokumentacji w ramach wdrożenia SZBI

1. Liczba jednostek objętych zadaniem: 1 (Urząd Miejski w Poniatowej)
2. Obecny stan dokumentacji SZBI: Wymagane jest opracowanie nowych polityk oraz aktualizacja istniejącej dokumentacji.
3. Podział dokumentacji: Wymagany jest podział dokumentacji na 4 części (Polityka Bezpieczeństwa Informacji, Polityka Bezpieczeństwa Danych Osobowych, Polityka Bezpieczeństwa Systemów Informatycznych, Polityka Bezpieczeństwa Fizycznego)
4. Obszary które powinny zostać objęte szczególnym uwzględnieniem w dokumentacji:
   a) Cel i zakres polityk w kontekście bezpieczeństwa informacji (BI);
   b) Role i odpowiedzialności pracowników w zakresie BI;
   c) Zarządzanie ryzykiem w obszarze BI;
   d) Procedury zarządzania incydentami BI;
   e) Deklarację stosowania zabezpieczeń;
   f) Kontrole dostępu do informacji i zasobów;
   g) Procedury związane z tworzeniem i prowadzeniem aktyw informacyjnych;
   h) Zasady pracy na odległość i mobilny dostęp do informacji;
   i) Bezpieczeństwo fizyczne pomieszczeń i obiektów związanych z BI;
   j) Bezpieczeństwo fizyczne nośników informacji;
   k) Bezpieczeństwo infrastruktury wspomagającej;
   l) Inwentaryzacja systemów informacyjnych;
   m) Zarządzanie bezpieczeństwem łańcucha dostaw w kontekście BI;
   n) Zarządzanie ciągłością działania systemów informatycznych w kontekście BI;
   o) Projektowanie i wdrażanie systemów teleinformatycznych;
   p) Kopie zapasowe;
   q) Sprzęt komputerowy, oprogramowanie strategiczne systemy i aplikacje;
   r) Serwery, informatyczna sieć wewnętrzna;

s) Rozliczalność działań w systemach informatycznych;
t) Procedury uwzględnienia BI w procesach planowania i zarządzania ciągłością działania;
u) Procedury bezpieczeństwa informacji w relacjach z dostawcami;
v) Okresowe szkolenia i podnoszenie świadomości pracowników z zakresu BI;
w) Cykliczne audyty i monitorowanie SZBI;
x) Procedury stosowania kryptografii i szyfrowania.

5. Dokumentacja musi zostać opracowana z uwzględnieniem przepisów RODO, ISO 27001, ustawy o krajowym systemie cyberbezpieczeństwa, rozporządzenia w sprawie krajowych ram interoperacyjności oraz wymaganiami dyrektywy NIS2
6. Indywidualizacja dokumentacji Dokumentacja musi być opracowana z uwzględnieniem wymagań i potrzeb stron zainteresowanych (wewnętrznych i zewnętrznych), indywidualnie oraz musi być opracowana na podstawie przepisów oraz informacji udzielonych przez pracowników podczas spotkań projektowych.
7. Wymagania dotyczące spotkań projektowych: Liczba spotkań projektowych wynosi minimum 2-3 udokumentowane spotkania z kadrą kierowniczą. Spotkania te mają na celu zebranie informacji niezbędnych do opracowania indywidualnych procedur oraz omówienie specyficznych potrzeb i wymagań Urzędu.

9) OPIS PRZEDMIOTU ZAMÓWIENIA dla zadania nr 3

1. Szczegółowe wymagania dotyczące szkoleń z zakresu bezpieczeństwa informacji

1.1 Zakres i cel szkoleń:
- 1.1.1 Szkolenie będzie obejmowało szczegółowe omówienie opracowanej dokumentacji SZBI.
- 1.1.2 Celem szkoleń jest zwiększenie świadomości pracowników, zapewnienie zgodności z przepisami oraz wdrożenie nowych procedur bezpieczeństwa informacji.
- 1.1.3 Szkolenia obejmują tematykę związaną z RODO, bezpieczeństwem informacji, zarządzaniem incydentami, korzystaniem z urządzeń mobilnych, postępowaniem z nośnikami danych, kontrolą dostępu, zabezpieczaniem pomieszczeń i obiektów, czystym biurkiem, czystym ekranem, wykonywaniem kopii zapasowych, ochroną logów, bezpieczeństwem komunikacji, zarządzaniem bezpieczeństwem sieci, przesyłaniem informacji, opracowywaniem planów ciągłości działania, zarządzaniem incydentami bezpieczeństwa informacji, ochroną danych osobowych, szacowaniem ryzyka w obszarze bezpieczeństwa informacji oraz okresowymi szkoleniami personelu.

1.2 Liczba uczestników i grup szkoleniowych:
- 1.2.1 Całkowita liczba uczestników: 50 pracowników
- 1.2.2 Liczba grup szkoleniowych: Minimum 3-4 grupy aby uniknąć dezorganizacji normalnej pracy.
- 1.2.3 Podział na grupy: Kadra zarządzająca, pracownicy administracyjni i techniczni oraz pozostali pracownicy.
- 1.2.4 Maksymalna liczba uczestników w jednej grupie: 20 osób.

1.3 Forma szkoleń:
- 1.3.1 Szkolenia stacjonarne w siedzibie Urzędu.
- 1.3.2 Metody szkoleniowe: wykłady, warsztaty, ćwiczenia praktyczne.
- 1.3.3 Czas trwania szkolenia dla jednej grupy: 3 - 4 godziny.
- 1.3.4 Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.

1.4 Materiały szkoleniowe:
- 1.4.1 Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
- 1.4.2 Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.

1.5 Wymagania dotyczące wykonawcy

1.5.1 Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z zakresu bezpieczeństwa informacji.
1.5.2 Preferowane certyfikaty i akredytacje trenerów.
1.5.3 Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.

1.6 Konspekt szkolenia:
1.6.1 Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
1.6.2 Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia

1.7 Ewaluacja szkoleń:
1.7.1 Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
1.7.2 Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
1.7.3 Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
1.7.4 Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
1.7.5 Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.

10) OPIS PRZEDMIOTU ZAMÓWIENIA dla zadania nr 4

1. Szczegółowe wymagania dotyczące szkoleń z zakresu cyberbezpieczeństwa

1.1 Zakres i cel szkoleń:
1.1.1 Celem szkoleń jest zwiększenie świadomości zagrożeń, edukowanie uczestników o aktualnych zagrożeniach cybernetycznych, takich jak phishing, ransomware, malware, ataki DDoS i inne rodzaje cyberataków. Zrozumienie, jak te zagrożenia mogą wpływać na organizację oraz jakie mogą być konsekwencje ich wystąpienia.
1.1.2 Minimalny zakres tematyczny szkoleń musi nawiązywać do wprowadzenia do zagadnień związanych z cyberbezpieczeństwem, zarządzanie incydentami bezpieczeństwa cyfrowego, ochrona przed zagrożeniami cyfrowymi, bezpieczeństwo sieci i infrastruktury IT, zarządzanie hasłami i uwierzytelnianiem, bezpieczne korzystanie z urządzeń mobilnych , postępowanie z nośnikami danych, tworzenie i zarządzanie kopiami zapasowymi, ochrona logów systemowych, zarządzanie bezpieczeństwem sieci, przesyłanie informacji, szacowanie ryzyka w obszarze bezpieczeństwa informacji

1.2 Liczba uczestników i grup szkoleniowych:
1.2.1 Całkowita liczba uczestników: 50 pracowników
1.2.2 Liczba grup szkoleniowych: Minimum 3-4 grupy aby uniknąć dezorganizacji normalnej pracy.
1.2.3 Maksymalna liczba uczestników w jednej grupie: 20 osób.

1.3 Forma szkoleń:
1.3.1 Szkolenia stacjonarne w siedzibie Urzędu.
1.3.2 Metody szkoleniowe: Wykłady, warsztaty, ćwiczenia praktyczne.
1.3.3 Czas trwania szkolenia dla jednej grupy: 3 - 4 godziny.
1.3.4 Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.

1.4 Materiały szkoleniowe:
1.4.1 Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
1.4.2 Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.

1.5 Wymagania dotyczące kwalifikacji trenerów:
- 1.5.1 Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z cyberbezpieczeństwa.
- 1.5.2 Preferowane certyfikaty i akredytacje trenerów.
- 1.5.3 Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.

1.6 Konspekt szkolenia:
- 1.6.1 Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
- 1.6.2 Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia

1.7 Ewaluacja szkoleń:
- 1.7.1 Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
- 1.7.2 Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
- 1.7.3 Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
- 1.7.4 Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
- 1.7.5 Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.

11) OPIS PRZEDMIOTU ZAMÓWIENIA dla zadania nr 5

1. Szczegółowe wymagania dotyczące audytu końcowego:

1.1 Liczba jednostek objętych audytami końcowymi: 1 (Urząd Miejski w Poniatowej).

1.2 Miejsce przeprowadzenia audytu końcowego: Siedziba Urzędu Miejskiego w Poniatowej

1.3 Zakres audytu końcowego:
- 1.3.1 Ocena poziomu bezpieczeństwa organizacyjnego związanego z posiadaną dokumentacją i procedurami.
- 1.3.2 Ocena poziomu bezpieczeństwa technicznego związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
- 1.3.3 Przeprowadzenie testów obejmujących konfigurację zakupionych w ramach projektu grantowego urządzeń i oprogramowania zwiększającego poziom bezpieczeństwa cyfrowego.

1.4 Zakres przeprowadzanych audytów na podstawie przepisów:
- 1.4.1 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.
- 1.4.2 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
- 1.4.3 Ustawa o krajowym systemie cyberbezpieczeństwa.
- 1.4.4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
- 1.4.5 Normy ISO 27001.

1.5 Raport z audytu końcowego musi zawierać co najmniej informacje o tym jak zakupy w ramach projektu wpłynęły na poprawę bezpieczeństwa informacji i cyberbezpieczeństwa w Urzędzie.

1.6 Forma przekazania i omówienia raportu: Spotkanie w siedzibie Urzędu, podczas którego wyniki audytu zostaną omówione z kadrą kierowniczą.