

ING.271.1.1.2025.GB

Opis przedmiotu zamówienia

1) ZAMÓWIENIE OBEJMUJE 5 ZADAŃ DO WYKONANIA:

Zadanie 1: Wykonanie audytów wstępnych:

1. Przeprowadzenie audytu wstępnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie;
2. Przeprowadzenie 9 audytów wstępnych Systemu Zarządzania Bezpieczeństwem Informacji w podległych jednostkach samorządu terytorialnego (JST);

Zadanie 2: Opracowanie nowych polityk i aktualizacja dokumentacji w ramach wdrożenia SZBI:

1. Opracowanie nowych polityk i aktualizacja dokumentacji w ramach opracowania i wdrożenia SZBI w Urzędzie;
2. Opracowanie nowych polityk i aktualizacja dokumentacji w ramach opracowania i wdrożenia SZBI w 9 podległych jednostkach.

Zadanie 3: Szkolenia z zakresu bezpieczeństwa informacji;

1. Przeprowadzenie szkoleń z zakresu bezpieczeństwa informacji oddzielnie:
 - 1.1: dla kadry zarządzającej Urzędu;
 - 1.2: dla pozostałych pracowników Urzędu;
2. Przeprowadzenie 9 szkoleń z zakresu bezpieczeństwa informacji oddzielnie :
 - 2.1: dla kadry zarządzającej jednostek podległych;
 - 2.2: dla pozostałych pracowników podległych jednostek samorządu terytorialnego;

Zadanie 4: Szkolenia z zakresu cyberbezpieczeństwa

1. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu;
2. Przeprowadzenie 9 szkoleń z zakresu cyberbezpieczeństwa dla pracowników podległych jednostek samorządu terytorialnego.

Zadanie 5: Wykonanie audytów końcowych.

1. Przeprowadzenie audytu końcowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie;
2. Przeprowadzenie 9 audytów końcowych Systemu Zarządzania Bezpieczeństwem Informacji w podległych jednostkach samorządu terytorialnego (JST).

2) Liczba jednostek objętych zamówieniem 10 jednostek (Urząd oraz 9 podległych JST).

1. Urząd Gminy Wojcieszków

Jednostki podległe JST:

1. Żłobek Gminny „PUCHATEK”
2. Centrum Usług Społecznych w Wojcieszkanie
3. Szkoła Podstawowa w Oszczepalinie
4. Szkoła Podstawowa w Siedliskach
5. Szkoła Podstawowa w Hermanowie
6. Szkoła Podstawowa w Woli Bystrzyckiej
7. Szkoła Podstawowa w Wólce Domaszewskiej
8. Szkoła Podstawowa w Wojcieszkanie
9. Przedszkole w Wojcieszkanie

3) Liczba osób objętych szkoleniem:

- Urząd Gminy Wojcieszków – łącznie 30 osób
- Jednostki podległe JST – łącznie 40 osób

- 4) Ilość stacji roboczych: 150 szt.
- 5) Ilość serwerów: 2 szt.
- 6) Ilość urządzeń sieciowych: 200 szt.
- 7) **OPIS PRZEDMIOTU ZAMÓWIENIA dla zadania nr 1:**

1. Szczegółowe wymagania dotyczące audytów wstępnych:

1.1. Liczba jednostek objętych audytami wstępnymi: 10 (Urząd oraz 9 podległych JST).

1.2. Miejsce przeprowadzenia audytów: Urząd Gminy oraz siedziba każdej jednostki.

1.3. Zakres audytów wstępnych:

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 przeprowadzanych audytów 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 Raporty z audytów wstępnych muszą zawierać informacje o stanie aktualnym, stwierdzonych uchybieniach oraz zalecenia pokontrolne

1.6 Forma przekazania i omówienia raportów: Spotkania w siedzibach każdej JST, podczas których wyniki audytów 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 zamówieniem 10 jednostek (Urząd oraz 9 podległych JST).

2) Obecny stan dokumentacji SZBI: Wymagane jest opracowanie nowych polityk oraz aktualizacja istniejącej dokumentacji.

a. Podział dokumentacji: Wymagany jest podział dokumentacji na 4 części (Polityka Bezpieczeństwa Informacji, Polityka Bezpieczeństwa Danych Osobowych, Polityka Bezpieczeństwa Systemów Informatycznych, Polityka Bezpieczeństwa Fizycznego)

b. 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 i ciągłością działania łańcuch dostaw;
 - n) Projektowanie i wdrażanie systemów teleinformatycznych;
 - o) Kopie zapasowe i zarządzanie ciągłością działania;
 - p) Sprzęt komputerowy, oprogramowanie strategiczne systemy i aplikacje;
 - q) Serwery, informatyczna sieć wewnętrzna;
 - r) Rozliczalność działań w systemach informatycznych;
 - s) Procedury uwzględnienia BI w procesach planowania i zarządzania ciągłością działania;
 - t) Procedury bezpieczeństwa informacji w relacjach z dostawcami;
 - u) Okresowe szkolenia i podnoszenie świadomości pracowników z zakresu BI;
 - v) Cykliczne audyty i monitorowanie SZBI.
- 3) Dokumentacja zostanie opracowana z uwzględnieniem przepisów:
- a) 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 (Dz.U. z 2024 r., poz. 773)
 - b) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077)
 - c) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).
 - d) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
 - e) i/lub zgodność z ISO/IEC 27001
- 4) Indywidualizacja dokumentacji Dokumentacja musi być opracowana z uwzględnieniem wymagań i potrzeb stron zainteresowanych (wewnętrznych i zewnętrznych), indywidualnie dla każdej jednostki i opracowana na podstawie przepisów oraz informacji udzielonych przez pracowników podczas spotkań projektowych.
- 5) Wymagania dotyczące spotkań projektowych Liczba spotkań projektowych w każdej jednostce 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 każdej jednostki.

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: Pracownicy 10 jednostek (Urząd oraz 9 podległych JST).
 - 1.2.2 Liczba grup szkoleniowych: Minimum 2-3 grupy na każdą jednostkę aby uniknąć dezorganizacji normalnej pracy każdej jednostki.
 - 1.2.3 Podział na grupy: Kadra zarządzająca oraz pracownicy administracyjni i techniczni.
 - 1.2.4 Maksymalna liczba uczestników w jednej grupie: 20 osób.
- 1.3 Forma szkoleń:
 - 1.3.1 Szkolenia stacjonarne w siedzibach każdej jednostki oraz 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: Pracownicy 10 jednostek (Urząd oraz 9 podległych JST).
- 1.2.2 Liczba grup szkoleniowych: Minimum 2-3 grupy na każdą jednostkę aby uniknąć dezorganizacji normalnej pracy każdej jednostki.
- 1.2.3 Maksymalna liczba uczestników w jednej grupie: 20 osób.

1.3 Forma szkoleń:

- 1.3.1 Szkolenia stacjonarne w siedzibach każdej jednostki oraz 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 audytów końcowych:
 - 1.1 Liczba jednostek objętych audytami końcowymi: 10 (Urząd oraz 9 podległych JST).
 - 1.2 Miejsce przeprowadzenia audytów końcowych: Urząd Gminy oraz siedziba każdej jednostki.
 - 1.3 Zakres audytów końcowych:
 - 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 Raporty z audytów końcowych muszą zawierać co najmniej informacje o tym jak zakupy w ramach projektu wpłynęły na poprawę bezpieczeństwa informacji i cyberbezpieczeństwa w jednostce.
 - 1.6 Forma przekazania i omówienia raportów: Spotkania w siedzibach Urzędu oraz podległych JST, podczas których wyniki audytów zostaną omówione z kadrą kierowniczą.