

## OPIS PRZEDMIOTU ZAMÓWIENIA

**Przedmiotem zamówienia jest Wykonanie audytu przedwdrożeniowego, audytu bezpieczeństwa systemów operacyjnych, opracowanie i wdrożenie wspólnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Gminy Sobienie-Jeziory, według najnowszej obowiązującej normy PN-EN ISO/IEC 27001:2023 oraz przeprowadzenie szkoleń z zakresu wdrażanego SZBI, cyberbezpieczeństwa i socjotechniki, w ramach konkursu grantowego "Cyberbezpieczny Samorząd"**

Przedmiotem zamówienia objęte są jednostki:

1. Urząd Gminy Sobienie-Jeziory, ul. Garwolińska 16, 08-443 Sobienie-Jeziory;
2. Gminny Ośrodek Pomocy Społecznej w Sobieniach- Jeziorach, ul. Garwolińska 16a, 08-443 Sobienie-Jeziory;
3. Zespół Szkół w Sobieniach-Jeziorach, ul. Garwolińska 14, 08-443 Sobienie-Jeziory;
4. Publiczna Szkoła Podstawowa w Warszawicach, Warszawice 13, 08-443 Sobienie-Jeziory;
5. Publiczna Szkoła Podstawowa w Siedzowie, Siedzów 30A, 08-443 Sobienie-Jeziory.

**Zamawiający przewiduje w ramach przedmiotu zamówienia następujące etapy realizacji:**

### **1) WYKONANIE AUDYTU PRZEDWDROŻENIOWEGO ORAZ AUDYTU BEZPIECZEŃSTWA SYSTEMÓW INFORMACYJNYCH**

#### **1. Kontekst, założenia dotyczące zamówienia**

- 1) Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Zamawiającego poprzez określenie do wdrożenia niezbędnych elementów Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami ujętymi w: ISO/IEC 27001:2022 (PN-ISO/IEC 27001:2023), PN- ISO/IEC 27005:2022, PN-ISO/IEC 22301:2020 wynikających z przepisów prawa, dla jednostek wskazanych powyżej.
- 2) Informacje ogólne o środowisku Zamawiającego:
  - a) Przetwarzanie informacji odbywa się według wskazanej wcześniej listy jednostek. Informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia około 160 osób.
  - b) Środowisko teleinformatyczne zawiera obecnie około 7 elementów aktywnych sieci, 3 serwery fizyczne, 6 serwerów wirtualnych, zlokalizowanych w jednostkach wskazanych w liście powyżej.
- 3) Zamawiający w ciągu 14 dni od dnia zawarcia Umowy prześle Wykonawcy dokumenty, którymi dysponuje w obszarze związanym z bezpieczeństwem informacji, w tym procedury wewnętrzne i wyniki przeprowadzonych audytów oraz szczegółową strukturę organizacyjną i informacje o środowisku teleinformatycznym, niezbędne do opracowania przez Wykonawcę wstępnego harmonogramu prac.

## 2. Zakres zamówienia

Usługa będzie obejmować swoim zakresem:

- 1) audyt przedwdrożeniowy u Zamawiającego;
- 2) audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług

### 1) Audyt przedwdrożeniowy

Audyt przedwdrożeniowy ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2023 przez Zamawiającego, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego, w wszystkich obszarach określonych załącznikiem A do ww. normy.

### 2) Audyt bezpieczeństwa systemów informacyjnych

Przeprowadzenie audytu bezpieczeństwa w oparciu o wymagania załącznika A do normy ISO 27001 oraz wytycznych normy ISO 27002 w zakresie bezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usług dla klientów jednostek.

Audyt powinien zawierać także wskazania podatności systemów informatycznych: wskazanie podatności, wagi podatności, opis podatności, informacje dotyczące podatności w tym źródła zewnętrzne, rekomendacje co do sposobu postępowania.

Wykonawca przy wykonywaniu umowy może, oprócz audytorów wskazanych w formularzu ofertowym, dodatkowo posiłkować się innymi pracownikami i współpracownikami Wykonawcy.

Powierzenie wykonania części przedmiotu Umowy innym pracownikom i współpracownikom nie wymaga uprzedniej zgody Zamawiającego, przy czym Wykonawca odpowiada za działania osób trzecich jak za działania własne.

Po zakończeniu audytu Wykonawca przygotowuje i przekazuje w formie elektronicznej oraz papierowej sprawozdanie z przeprowadzonego audytu.

## 3. Ogólne wymagania odnośnie do audytów

Audyty zostaną przeprowadzone w lokalizacjach jednostek Zamawiającego. Za zgodą Zamawiającego zdalnie można wykonywać czynności uzupełniające – np. przysyłanie materiałów lub wyjaśnień. Łączny czas trwania audytów nie może być krótszy niż 24 godziny robocze.

- Audyt Techniczny – według wymagań zawartych w załączniku A normy ISO/IEC 27001.
- Audyt Systemowy – według wymagań normy zawartych w normie ISO/IEC 27001.
- Sporządzenie raportów w formie pisemnej (edytowalnej i nieedytowalnej).
- Przekazanie raportów do Zamawiającego.
- Wykonanie razem z Zamawiającym działań poaudytowych, w formie uzgodnionej z Zamawiającym.

## **2) OPRACOWANIE I WDROŻENIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI ZGODNIE Z NORMĄ PN-EN ISO/IEC 27001**

Opracowanie przez Wykonawcę niżej wymienionych dokumentów, przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej do stanu, który pozwala przekazać dokumenty jednostce certyfikującej, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego. Po stronie Zamawiającego leży jedynie uzgodnienie treści dokumentów z Wykonawcą.

### **1) Klasyfikacja informacji przetwarzanych u Zamawiającego**

W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:

- opracowanie metodyki klasyfikowania informacji przetwarzanych u Zamawiającego;
- opracowanie modelu podziału informacji przetwarzanych u Zamawiającego w zależności od poziomu ich wrażliwości i przeznaczenia;
- sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych u Zamawiającego;
- opracowanie raportu z procesu klasyfikacji informacji.

### **2) Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego zgodnie z wytycznymi normy PN-ISO/IEC 27005:2022**

W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego, a w szczególności:

- opracować metodykę szacowania ryzyka spełniającą wymagania PN-ISO/IEC 27005:2022, optymalną ze względu na charakter działalności Zamawiającego;
- opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
- przeprowadzić wspólnie z wyznaczonymi pracownikami Zamawiającego proces szacowania ryzyka, w tym:
  - zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
  - opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Zamawiającego;
  - opracować przy współudziale wyznaczonych pracowników Zamawiającego plan

postępowania z ryzykiem.

### 3) Opracowanie dokumentów niezbędnych do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji

Opracowanie wraz z przekazaniem praw autorskich dokumentów niezbędnych do opracowania systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami:

- a) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
- b) 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,
- c) ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest przedstawić elementy niezbędne do uzupełniania w celu opracowania dokumentacji SZBI przez Zamawiającego, a także wytypować procesy niezbędne do poprawnego funkcjonowania organizacji. Dokument/y muszą ponadto stanowić szczegółowy wykaz dokumentów niezbędnych do opracowania na potrzeby SZBI z zaznaczeniem ich wzajemnych powiązań, w tym:

- Dokument Główny Polityki Zarządzania Bezpieczeństwem Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa, procesy, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
- Deklarację Stosowania wraz z odniesieniem do obecnie opracowywanych dokumentów;
- Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji u Zamawiającego, w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;
- Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

Wykonawca gwarantuje, że dokumentacja systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy ISO/IEC 27001 oraz wymaganiami certyfikacyjnymi jednostki certyfikującej systemy zarządzania na zgodność z normą ISO/IEC 27001, akredytowanej przez Polską jednostkę akredytującą wymienioną na stronie

[http://www.iaf.nu//articles/IAF\\_MEMBERS\\_SIGNATORIES/4](http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4).

W skład dokumentacji SZBI w szczególności wchodzi następujące polityki i procedury:

1. Polityka bezpieczeństwa informacji,
2. Księga systemu zarządzania bezpieczeństwem informacji,
3. Schemat organizacyjny kierowania sprawami bezpieczeństwa informacji,
4. Mapa procesów objętych SZBI minimum 6 procesów (min. proces zarządzania i utrzymania SZBI, proces zarządzania ryzykiem, proces zarządzania incydentami (RODO, UoKSC), proces



zarządzania dostawami (wybór-realizacja-zakończenie współpracy), proces zarządzania pracownikami (rekrutacja-zatrudnienie-zwolnienie), proces obsługi interesanta (obsługa wniosków). Schemat procesów należy przygotować w notacji BPMN (forma edytowalna),

5. Deklaracja stosowania zabezpieczeń dla systemu bezpieczeństwa informacji wraz z przyporządkowaniem aktualnie używanych w organizacji rozwiązań do wymagań normy,
6. Metodyka szacowania ryzyka zgodnie z wymaganiami normy ISO27005:2022,
7. Polityka i plany ciągłości działania (BCP) zgodny z wymaganiami określonymi w normie ISO22301:2019.
8. Wszystkie procedury potrzebne do przejścia procesu certyfikacji:
  - Procedura nadzoru nad dokumentami,
  - Procedura działań doskonalących, korygujących i zapobiegawczych,
  - Procedura audytu wewnętrznego,
  - Procedura nadzoru nad zapisami,
  - Procedura przeglądu zarządzania,
  - Procedura zarządzania incydentami,
  - Procedura bezpieczeństwa wewnętrznego organizacji,
  - Procedura ewakuacji personelu i sprzętu z obiektów,
  - Procedura klasyfikacji informacji wewnętrznych i zewnętrznych,
  - Procedura oceny ryzyk generowanych przez strony zewnętrzne (klientów, dostawców, kooperantów, innych),
  - Procedura postępowania w przypadku odejścia pracownika z firmy,
  - Procedura bezpieczeństwa infrastruktury teleinformatycznej (sieć, serwerownie, urządzenia łączności, inne elementy),
  - Procedura bezpieczeństwa fizycznego,
  - Procedura pomiaru skuteczności SZBI,
  - Dokumenty ustalające status systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy,
  - Opracowanie formularzy i rejestrów będących integralną częścią w/w dokumentów w formie i treści odpowiedniej do potrzeb i woli Zamawiającego (zawartość merytoryczna oraz forma),
  - Inne niezbędne u Zamawiającego z punktu widzenia systemu bezpieczeństwa informacji (po ocenie potrzeb).

#### 4) Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

- 1) Analiza ryzyka u Zamawiającego zgodnie z wymaganiami normy ISO27005:2022:
  - Identyfikacja aktywów informacyjnych,
  - Identyfikacja zagrożeń,
  - Identyfikacja i ocena podatności, które mogą być wykorzystane przez zagrożenia dla aktywów,

**na Rozwój Cyfrowy**

- Identyfikacja i ocena skutków utraty poufności, integralności i dostępności w odniesieniu do aktywów,
  - Ocena ryzyka.
- 2) Analiza ryzyka u Zamawiającego zgodnie z wymaganiami normy ISO222301(BIA).
- 3) Wdrożenie dokumentów do stosowania, a w szczególności:
- przygotowanie i przekazanie wytycznych odnośnie do elektronicznego nadzorowania dokumentów i zapisów, jeżeli potrzebne, konfiguracja ustawień,
  - uzupełnienia zapisów wymaganych normą razem z Zamawiającym,
  - konsultacje indywidualne z zakresu stosowania opracowanej dokumentacji,
  - udzielenie wszelkiego wsparcia w celu uzyskania biegłego posługiwania się przez Zamawiającego systemem (nie mniej niż 20 godzin).

**3) SZKOLENIE Z SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI****Szkolenie dla pracowników i kadry zarządzającej (ilość osób 160):**

- 1) Pracownicy powinni zdobyć wiedzę na temat zasad ochrony informacji w organizacji oraz roli, jaką pełnią w utrzymaniu i przestrzeganiu SZBI. Celem jest podniesienie świadomości dotyczącej bezpieczeństwa informacji, ryzyk związanych z ich przetwarzaniem oraz zagrożeń cybernetycznych. Kadra zarządzająca zdobędzie wiedzę o roli kierownictwa w zapewnieniu skutecznego zarządzania bezpieczeństwem informacji, umożliwiającą pełne wdrożenie i ciągłe doskonalenie SZBI w organizacji. Uczestnicy powinni zrozumieć swoje obowiązki związane z nadzorowaniem polityki bezpieczeństwa oraz wprowadzać działania zapewniające zgodność z normami i regulacjami.
- 2) **Zakres tematyczny:**
- **Podstawy SZBI:** Wprowadzenie do norm i standardów związanych z bezpieczeństwem informacji (np. ISO/IEC 27001, RODO, itp.), przegląd podstawowych pojęć związanych z bezpieczeństwem informacji, oraz znaczenie SZBI w kontekście organizacyjnym.
  - **Polityki bezpieczeństwa informacji:** Omówienie głównych polityk organizacji w zakresie ochrony danych i informacji.
  - **Ryzyka i zagrożenia:** Analiza typowych zagrożeń związanych z bezpieczeństwem informacji oraz technik wykorzystywanych przez cyberprzestępców.
  - **Procedury ochrony informacji:** Przedstawienie procedur dotyczących klasyfikacji, przetwarzania i przechowywania informacji w sposób bezpieczny.
  - **Rola pracownika w SZBI:** Zrozumienie odpowiedzialności pracowników za przestrzeganie zasad SZBI, w tym odpowiednie zarządzanie hasłami, szyfrowanie danych oraz zgłaszanie nieprawidłowości.
  - **Zarządzanie incydentami bezpieczeństwa:** Procedury postępowania w przypadku wykrycia incydentu związane z bezpieczeństwem informacji (np. ataków cybernetycznych, wycieków danych).
  - **Prawo i regulacje dotyczące ochrony danych i informacji:** Omówienie przepisów prawnych i regulacyjnych, które wpływają na zarządzanie danymi i informacjami w organizacji.

**na Rozwój Cyfrowy**

- **Rola kierownictwa w SZBI:** Omówienie odpowiedzialności osób zarządzających jednostką w zakresie wdrożenia, monitorowania i oceny skuteczności SZBI. Zrozumienie roli liderów w tworzeniu kultury bezpieczeństwa w organizacji.
  - **Planowanie i strategia SZBI:** Jak stworzyć i wdrożyć długoterminową strategię bezpieczeństwa informacji, uwzględniając cele biznesowe i ryzyka związane z bezpieczeństwem informacji.
  - **Zarządzanie ryzykiem w SZBI:** Zrozumienie procesów oceny, analizy i zarządzania ryzykiem bezpieczeństwa informacji. Omówienie narzędzi i metod służących identyfikowaniu zagrożeń oraz wdrażania działań zaradczych.
  - **Polityki i procedury:** Jak opracować i wdrożyć polityki bezpieczeństwa informacji oraz procedury operacyjne w zakresie ochrony danych i informacji. Przykłady polityk bezpieczeństwa, zarządzanie dostępem, zasady ochrony danych osobowych, zarządzanie incydentami.
  - **Zgodność z regulacjami:** Zrozumienie przepisów prawnych i regulacji, takich jak RODO, które mają wpływ na politykę bezpieczeństwa informacji w organizacji. Jak zapewnić zgodność z wymogami prawnymi oraz audyty wewnętrzne.
  - **Monitorowanie i audyt SZBI:** Nadzór nad monitorowaniem efektywności SZBI, w tym rola audytów wewnętrznych i zewnętrznych w utrzymaniu zgodności z wymaganiami. Jak przeprowadzać ocenę ryzyka i analizę bezpieczeństwa.
  - **Reagowanie na incydenty i ciągłość działalności:** Opracowanie planów reagowania na incydenty związane z bezpieczeństwem informacji. Jak stworzyć i wdrożyć plan ciągłości działania oraz plan odzyskiwania po awarii (disaster recovery).
  - **Doskonalenie SZBI:** Strategie wprowadzania ciągłych usprawnień w systemie zarządzania bezpieczeństwem informacji. Jak śledzić zmiany w technologii, przepisach prawnych i zagrożeniach, oraz dostosować SZBI do nowych wyzwań.
- 3) **Metodyka szkolenia:**
- **Wykłady teoretyczne:** Prezentacje i omówienie podstawowych zagadnień związanych z SZBI.
  - **Ćwiczenia praktyczne:** Przykłady realnych incydentów bezpieczeństwa, scenariusze i case study do analizy i rozwiązania.
  - **Dyskusje grupowe:** Wymiana doświadczeń i poglądów między uczestnikami, które mogą pomóc w lepszym zrozumieniu praktycznych aspektów bezpieczeństwa informacji.
  - **Testy wiedzy:** Po zakończeniu szkolenia uczestnicy powinni przejść test sprawdzający przyswojoną wiedzę.
- 4) **Forma szkolenia:**
- Szkolenie może odbywać się w formie **stacjonarnej** lub **online**, w czasie rzeczywistym (nagrania nie są dopuszczalne).
  - Wykonawca jest zobowiązany zapewnić materiały szkoleniowe dla każdego uczestnika (w formie papierowej lub elektronicznej).
- 5) **Organizacja i miejsce szkolenia:**
- Wykonawca zobowiązany jest zaproponować termin oraz miejsce szkolenia, do akceptacji przez Zamawiającego.
- 6) **Czas trwania:** Szkolenie powinno trwać co najmniej 8 godzin, z możliwością podziału na dwie sesje, np. po 4 godziny.
- 7) **Ocena efektywności szkolenia:** Po zakończeniu kursu należy ocenić poziom zrozumienia materiału przez uczestników, zarówno poprzez testy, jak i dyskusję. Warto także

przeprowadzić ewaluację szkolenia, aby ocenić jego użyteczność i dostosowanie do potrzeb pracowników.

8) **Zaświadczenia:** osoby uczestniczące w szkoleniu otrzymują zaświadczenia o ukończeniu szkolenia

#### 4) SZKOLENIE Z ZAKRESU CYBERBEZPIECZEŃSTWA I SOCJOTECHNIKI

**Szkolenie dla pracowników i kadry zarządzającej jednostek (ilość osób 160):**

##### 1) Cel szkolenia

Celem szkolenia jest podniesienie kompetencji uczestników w zakresie bezpieczeństwa informacji oraz cyberbezpieczeństwa, zakończone uzyskaniem certyfikatu potwierdzającego nabyte umiejętności. Uczestnicy powinni zdobyć praktyczne umiejętności oraz wiedzę umożliwiającą ochronę danych przetwarzanych w formie tradycyjnej i wykorzystaniem systemów informacyjnych. Szkolenie należy przeprowadzić dla pracowników następujących jednostek:

- Urząd Gminy Sobienie-Jeziory, ul. Garwolińska 16, 08-443 Sobienie-Jeziory,
- Gminny Ośrodek Pomocy Społecznej w Sobieniach-Jeziorach, ul. Garwolińska 16A, 08-443 Sobienie-Jeziory,
- Zespół Szkół w Sobieniach Jeziorach, ul. Garwolińska 14, 08-443 Sobienie-Jeziory,
- Publiczna Szkoła Podstawowa w Warszawicach, Warszawice 13, 08-443 Sobienie-Jeziory,
- Publiczna Szkoła Podstawowa w Siedzowie, Siedzów 30A, 08-443 Sobienie-Jeziory.

##### 2) Wymagania dotyczące szkolenia

###### Czas trwania:

Szkolenie powinno trwać minimum 8 godzin dydaktycznych (1 godzina dydaktyczna = 45 minut).

###### Forma szkolenia:

Szkolenie będzie realizowane w formie stacjonarnej

Miejsce szkolenia – Świetlica w Sobieniach-Jeziorach, ul. Duży Rynek 25, 08-443 Sobienie-Jeziory.

###### Podział na grupy:

Szkolenie zostanie zrealizowane w podziale na 6 grup, każda z grup będzie liczyła ok. 25 – 28 osób (łącznie ok. 160 osób).

###### Zakres szkolenia:

Szkolenie powinno swoim zakresem obejmować co najmniej poniżej wymienioną tematykę:

- Podstawy bezpieczeństwa informacji:
  - Definicja i znaczenie bezpieczeństwa informacji w jednostkach samorządu terytorialnego,
  - Podstawowe zasady ochrony informacji w administracji publicznej;
- Zarządzanie dostępem i tożsamością:
  - Tworzenie i zarządzanie bezpiecznymi hasłami,
  - Autoryzacja i uwierzytelnianie użytkowników - mechanizmy wieloskładnikowe;
- Rozpoznawanie i zapobieganie cyberzagrożeniom:
  - Phishing – jak rozpoznawać próby wyłudzenia danych,
  - Ransomware i inne rodzaje złośliwego oprogramowania,
  - Bezpieczne korzystanie z poczty elektronicznej i internetu;
- Bezpieczeństwo urządzeń i pracy sieci:
  - Zabezpieczanie urządzeń końcowych (komputery, telefony, tablety),
  - Bezpieczne korzystanie z sieci Wi-Fi,
  - Aktualizacje oprogramowania i systemów operacyjnych;



**na Rozwój Cyfrowy**

- Postępowanie w przypadku incydentów bezpieczeństwa:
  - Rozpoznawanie oznak naruszenia bezpieczeństwa,
  - Procedury zgłaszania incydentów,
  - Planowanie działań naprawczych po incydencie;
- Bezpieczna praca zdalna:
  - Ryzyka związane z pracą zdalną,
  - Zasady korzystania z narzędzi do pracy zdalnej,
  - Ochrona danych w środowisku domowym;
- Zasady bezpiecznego korzystania z systemów i aplikacji:
  - Bezpieczna obsługa systemów informatycznych,
  - Unikanie ryzyk związanych z korzystaniem z nieznanych aplikacji,
  - Aktualizacje systemów i ich znaczenie;
- Prawo i odpowiedzialność w zakresie bezpieczeństwa informacji:
  - Odpowiedzialność karna i cywilna za naruszenie zasad bezpieczeństwa,
  - Wytyczne krajowe i międzynarodowe dotyczące cyberbezpieczeństwa;
- Edukacja i budowanie świadomości użytkowników:
  - Znaczenie świadomości pracowników w budowaniu kultury bezpieczeństwa,
  - Przykłady incydentów i ich konsekwencji,
  - Narzędzia i materiały wspierające samodzielną naukę w zakresie cyberbezpieczeństwa.

**Certyfikacja:**

Uczestnicy szkolenia powinni otrzymać certyfikaty potwierdzające zdobycie kompetencji w zakresie przeprowadzonego szkolenia. Zamawiający oczekuje przeprowadzenia testu kompetencyjnego. Czas realizacji testu nie wchodzi w czas szkolenia.

**Organizacja i koszty:**

Zamawiający zapewni salę pozwalającą na przeprowadzenie szkolenia jednocześnie dla min. 25 osób. Wykonawca jest zobowiązany zapewnić materiały dydaktyczne i szkoleniowe dla przeprowadzenia szkolenia.

**Wymagania wobec Wykonawcy**

Wykonawca powinien posiadać minimum 3 letnie doświadczenie w zakresie przeprowadzania szkoleń z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa.

Wykonawca zobowiązany jest do przedłożenia szczegółowego harmonogramu i programu szkolenia przed jego rozpoczęciem.

**Warunki realizacji**

Zamawiający zastrzega sobie prawo do akceptacji propozycji Wykonawcy dotyczących terminu realizacji szkolenia.

Szkolenie musi zostać zrealizowane zgodnie z zaakceptowanym harmonogramem i programem.

**Wymagania dla firmy oraz osób realizujących przedmiot zamówienia:****Certyfikaty i doświadczenie firmy:**

- 1) Wykonawca ubiegający się o zamówienie powinien wykazać się certyfikowanym systemem SZBI zgodnie z normą ISO27001, utrzymanym od co najmniej 3 lat,

**na Rozwój Cyfrowy**

- 2) Wykonawca musi wykazać co najmniej 2 wdrożenia SZBI wg normy ISO27001 wykonane w podmiotach publicznych,
- 3) Wykonawca przeprowadził co najmniej 4 audyty na rzecz podmiotów publicznych w zakresie SZBI zgodnego z wymaganiami normy ISO27001 w ostatnich 3 latach (należy przedstawić wykaz audytów).

**Certyfikacje i doświadczenie zawodowe osób realizujących zamówienie**

Co najmniej dwie osoby z zespołu opracowująca SZBI powinny posiadać ważny przez okres realizacji umowy co najmniej jeden z certyfikatów, które potwierdzają ich kompetencje w zakresie bezpieczeństwa informacji:

- **ISO 27001 Lead Implementer:** certyfikat potwierdzający umiejętności w zakresie wdrażania SZBI zgodnie z normą ISO 27001; lub
- **ISO 27001 Lead Auditor:** certyfikat potwierdzający umiejętności przeprowadzania audytów systemów zarządzania bezpieczeństwem informacji; lub
- **CISM (Certified Information Security Manager):** certyfikat dla osób zarządzających bezpieczeństwem informacji; lub
- **CISSP (Certified Information Systems Security Professional):** certyfikat dotyczący profesjonalnego zarządzania bezpieczeństwem informacji.

Kierownik zespołu wdrażającego powinien wykazać się udziałem w co najmniej 2 wdrożeniach SZBI w podmiotach publicznych oraz co najmniej 1 z certyfikatów wymienionych powyżej.