Załącznik nr 1

**Opis przedmiotu zamówienia**

# Szkolenie z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) – szkolenie dla pracowników

1. Przedmiot zamówienia
Przedmiotem zamówienia jest organizacja i przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji oraz funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), skierowanego do pracowników Zamawiającego.

Szkolenie ma na celu podniesienie świadomości personelu w zakresie ochrony informacji, zagrożeń, obowiązków pracowniczych wynikających z przepisów prawa oraz norm i stadardów.

1. Grupa docelowa
Szkolenie skierowane jest dla pracowników merytorycznych urzędu.

Liczba uczestników: 109 osób.

1. Cel szkolenia
Celem szkolenia jest:
* podniesienie świadomości zagrożeń dla bezpieczeństwa informacji,
* zapoznanie uczestników z zasadami ochrony danych i informacji w codziennej pracy,
* wskazanie odpowiedzialności i obowiązków pracowników wynikających z przepisów prawa i polityk wewnętrznych,
* minimalizacja ryzyka błędów pracowniczych prowadzących do incydentów bezpieczeństwa,
* przygotowanie pracowników do prawidłowego reagowania na sytuacje naruszenia bezpieczeństwa informacji.
1. Zakres tematyczny szkolenia
Program szkolenia obejmuje co najmniej:

4.1. Podstawowe pojęcia bezpieczeństwa informacji:

* Co to jest bezpieczeństwo informacji?
* Dane osobowe, informacje poufne, dane finansowe — co chronimy?
* Przykłady naruszeń bezpieczeństwa i ich konsekwencje.

4.2. Obowiązki pracowników wynikające z SZBI i przepisów prawa:

* Obowiązki wynikające z ISO/IEC 27001.
* Obowiązki wynikające z RODO i przepisów ochrony danych osobowych.
* Odpowiedzialność pracownika za naruszenie zasad ochrony informacji.

4.3. Codzienne dobre praktyki:

* Bezpieczne logowanie, zarządzanie hasłami.
* Ochrona komputerów i urządzeń mobilnych.
* Ochrona dokumentów papierowych.
* Czyste biurko i ekran — Clean Desk & Clean Screen Policy.
* Korzystanie z poczty elektronicznej i Internetu w sposób bezpieczny.

4.4. Zagrożenia bezpieczeństwa:

* Phishing, socjotechnika, próby oszustw.
* Złośliwe oprogramowanie i nieautoryzowane oprogramowanie.
* Błędy pracownicze jako źródło incydentów.

4.5. Incydenty bezpieczeństwa informacji:

* Co to jest incydent bezpieczeństwa?
* Obowiązek zgłaszania incydentów i podejrzanych sytuacji.
* Procedura postępowania w przypadku naruszenia bezpieczeństwa.
1. Forma realizacji szkolenia
* Szkolenie realizowane będzie w formie:
	+ online
* Czas trwania szkolenia: minimum 6 godzin dydaktycznych.
* Forma prowadzenia: wykład z elementami warsztatowymi, omówienie przykładów praktycznych.
* Zapewnienie materiałów szkoleniowych w formie elektronicznej.
* Potwierdzenie udziału uczestników (lista obecności) dopuszcza się w formie elektronicznej.
* Imienne zaświadczenia ukończenia szkolenia dla uczestników.
1. Wymagania wobec Wykonawcy
* Doświadczenie w prowadzeniu szkoleń z zakresu bezpieczeństwa informacji, RODO, ISO/IEC 27001.
* Minimum 2-letnie doświadczenie w realizacji szkoleń dla administracji publicznej, jednostek sektora finansów publicznych lub sektora prywatnego.
* Preferowane posiadanie przez wykładowcę certyfikatów z zakresu bezpieczeństwa informacji (np. ISO/IEC 27001 LA i wykształcenia wyższego informatycznego.
1. Termin realizacji
* Termin wykonania zamówienia: do uzgodnienia, nie później niż od wrześnie 2025r do marca 2026r.

# Szkolenie z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) – szkolenie dla kadry kierowniczej

1. Przedmiot zamówienia Przedmiotem zamówienia jest organizacja i przeprowadzenie specjalistycznego szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) skierowanego do kadry zarządzającej Zamawiającego, obejmującego w szczególności osoby pełniące funkcje decyzyjne w zakresie zarządzania organizacją, ryzykiem oraz bezpieczeństwem informacji.
2. Grupa docelowa Szkolenie przeznaczone jest dla:
* kadry kierowniczej wyższego i średniego szczebla,
* członków zarządu, dyrektorów, kierowników działów,
* właścicieli procesów biznesowych, właścicieli aktywów informacyjnych,
* pełnomocnika ds. SZBI (jeżeli wyznaczony).

Planowana liczba uczestników: 20 osób.

1. Cel szkolenia

Celem szkolenia jest:

* przedstawienie roli i odpowiedzialności kierownictwa w funkcjonowaniu SZBI,
* omówienie obowiązków zarządczych wynikających z normy ISO/IEC 27001:2022, przepisów prawa i wymogów regulatorów,
* przekazanie wiedzy niezbędnej do podejmowania decyzji w zakresie zarządzania ryzykiem i bezpieczeństwem informacji,
* podniesienie świadomości strategicznej w zakresie cyberbezpieczeństwa, ciągłości działania i zarządzania incydentami.
1. Zakres tematyczny szkolenia Program szkolenia obejmuje m.in.:

4.1. Podstawowe założenia SZBI

* Czym jest System Zarządzania Bezpieczeństwem Informacji (ISO/IEC 27001:2022).
* Kluczowe role i odpowiedzialności kierownictwa.
* Korzyści biznesowe z wdrożenia SZBI.

4.2. Wymagania zarządcze w SZBI

* Przywództwo i zobowiązanie kierownictwa (punkt 5 normy ISO/IEC 27001:2022).
* Polityka bezpieczeństwa informacji i cele SZBI.
* Przydzielanie odpowiedzialności i uprawnień.

4.3. Zarządzanie ryzykiem bezpieczeństwa informacji

* Rola kierownictwa w akceptacji ryzyk.
* Procesy szacowania i akceptacji ryzyka (ISO/IEC 27005:2022).
* Budowa apetytu na ryzyko organizacji.

4.4. Zgodność i wymagania prawne

* Odpowiedzialność kadry zarządzającej za zapewnienie zgodności (compliance).
* Obowiązki wynikające z przepisów prawa: RODO, NIS2, krajowy system cyberbezpieczeństwa, inne akty normatywne w zależności od specyfiki organizacji.

4.5. Odpowiedzialność zarządcza za incydenty i nadzór nad systemem

* Rola kierownictwa w zarządzaniu incydentami bezpieczeństwa.
* Raportowanie do zarządu i organów nadzorczych.
* Monitorowanie skuteczności SZBI i decyzje strategiczne.
1. Forma realizacji szkolenia
* Szkolenie realizowane będzie w formie:
	+ online
* Czas trwania szkolenia: minimum 6 godzin dydaktycznych.
* Forma prowadzenia: wykład ekspercki z elementami dyskusji i case study.
* Zapewnienie materiałów szkoleniowych w formie elektronicznej i/lub papierowej.
* Potwierdzenie udziału uczestników (lista obecności) dopuszcza się w formie elektronicznej.
* Imienne zaświadczenia ukończenia szkolenia dla uczestników.