

Załącznik nr 1 do SWZ – Szczegółowy opis przedmiotu zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

Opracowanie dokumentacji SZBI, przeprowadzenie audytu bezpieczeństwa oraz szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy Susiec

Zadanie 1 – SZKOLENIA

1. Szkolenia kadry w zakresie cyberbezpieczeństwa

Szkolenie dla pracowników administracyjnych w zakresie cyberbezpieczeństwa. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych. Szkolenie stacjonarne z zakresu cyberbezpieczeństwa skierowane jest do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

- a. Podstawowe zagrożenia związane z korzystaniem z Internetu: wirusy, phishing, ransomware, poczta e-mail, strony www, serwisy społecznościowe,
- b. Reguły tworzenia i zmiany haseł do systemów informatycznych i aplikacji,
- c. Bezpieczeństwo urządzeń mobilnych,
- d. Zabezpieczanie informatycznych nośników danych – pendrive, pamięci zewnętrzne,
- e. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia,
- f. Prawidłowe korzystanie z oprogramowania antywirusowego i zapory ogniowej,
- g. Zasady instalacji i aktualizacji programów oraz aplikacji,
- h. Przedstawienie najczęściej spotykanych, aktualnych ataków na użytkowników,
- i. Realizacja testu sprawdzającego wiedzę uczestników po szkoleniu.

Przewiduje się, że szkolenie potrwa minimum 3 godziny dla jednej grupy. Zajęcia będą organizowane w 2 grupach szkoleniowych po ok. 15 pracowników, a po zakończeniu zajęć każdej grupy przewidziano sesję pytań i odpowiedzi z uczestnikami.

W ramach organizacji szkolenia Wykonawca musi zapewnić:

- a. Materiały szkoleniowe.
- b. Kadrę trenerską posiadającą wiedzę, min. 2 – letnie doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia
- c. Prowadzenie dokumentacji – lista obecności, certyfikaty uczestnictwa.

Zadanie 2 - OPRACOWANIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI) ORAZ AUDYT KOŃCOWY

Przedmiotem niniejszego zadania jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania PN-EN ISO/IEC 27001:2023-08 w zakresie bezpieczeństwa informacji dla Urzędu Gminy Susiec oraz audyt wdrożonego SZBI.

2. Wymagania formalne i merytoryczne

Wykonawca zobowiązany jest do opracowania spójnej, jednolitej i adekwatnej do faktycznych ryzyk, procesów oraz potrzeb Zamawiającego dokumentacji SZBI oraz BCM, zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023-08

Celem wdrożenia jest zapewnienie wysokiego poziomu bezpieczeństwa informacji oraz spełnienie wymagań:

- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. poz. 773),
- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) (Dz. Urz. UE L 119 z 04.05.2016, str. 1),
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781),
- Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557, z późn. zm.),
- Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632, z późn. zm.),
- Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, z późn. zm.),
- Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 (dyrektywa NIS 2).

3. Szczegółowy opis przedmiotu zamówienia

- Poprzez opracowanie dokumentacji systemu należy rozumieć: przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej do stanu, który pozwala przekazać dokumenty do jednostki certyfikującej przez Zamawiającego, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego.
- Wykonawca na etapie prac wdrożeniowych uzgadnia treść dokumentów z Zamawiającym.
- Wykonawca gwarantuje, że dokumentacja systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy PN-EN ISO/IEC 27001:2023-08
- Zamawiający udostępnia Wykonawcy wszystkie niezbędne materiały i udzieli odpowiedzi na pytania podczas realizacji przedmiotu zamówienia.
- Wykonawca zobowiązany jest do zachowania w poufności informacji uzyskanych na etapie opracowania i wdrożenia SZBI u Zamawiającego.
- Zamawiający wymaga, aby dokumentacja SZBI była utworzona zgodnie z obowiązującymi przepisami prawa oraz najlepszymi praktykami.
- Wsparcie powdrożeniowe w wymiarze 16 godzin roboczych po zakończeniu wdrożenia (konsultacje, pomoc w aktualizacji dokumentacji, wsparcie przy audycie zewnętrznym).
- Poprzez wdrożenie należy rozumieć utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego oraz przeprowadzenie instruktażu w zakresie

wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

4. Wymagania dotyczące dokumentacji

- Wymagane jest odniesienie do wszystkich celów stosowania zabezpieczeń, o których mowa w załączniku A do normy ISO PN-EN ISO/IEC 27001:2023-08 w postaci mapowania: wymaganie załącznika A -> zabezpieczenie.
- Opracowane polityki, procedury itd. muszą realnie odnosić się do procesów u Zamawiającego.
- Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem zrozumiałym dla osób nie posiadających wysokiego przygotowania z zakresu bezpieczeństwa informacji.

5. Etapy realizacji usługi

Etap I. Opracowanie niezbędnej dokumentacji SZBI

- Polityka bezpieczeństwa informacji – określenie celów, zasad i odpowiedzialności w zakresie bezpieczeństwa informacji.
- Instrukcje zarządzania systemem informatycznym – opis zarządzania i monitorowania systemu IT.
- Opis przepływu informacji – przedstawienie sposobu przepływu danych między systemami.
- Instrukcje postępowania w sytuacjach naruszenia ochrony danych osobowych.
- Deklaracja stosowania – obejmująca polityki bezpieczeństwa oraz zgodność z normą PN-EN ISO/IEC 27001:2023-08.
- Podręcznik bezpieczeństwa informacji – szczegółowy dokument opisujący zasady SZBI.
- Metody analizy ryzyka – określenie i ocena ryzyk związanych z bezpieczeństwem informacji.
- Plan ciągłości działania – procedury przywracania kluczowych procesów biznesowych po incydencie bezpieczeństwa.
- Klasyfikacja informacji – zasady klasyfikacji danych według poziomu wrażliwości.
- Zarządzanie uprawnieniami – procedury nadawania, zmiany i rejestrowania uprawnień do przetwarzania danych w systemach IT.
- Zarządzanie bezpieczeństwem fizycznym i dostępem do pomieszczeń.
- Zarządzanie bezpieczeństwem fizycznym sprzętu i nośników.
- Użytkowanie stanowiska komputerowego – zasady bezpiecznej pracy.
- Zarządzanie incydentami – procedury zgłaszania, analizy i rozwiązywania incydentów.
- Procedura zarządzania zmianami – zasady wprowadzania zmian w systemach i procesach.
- Ochrona danych osobowych – procedury zgodne z RODO.
- Procedura implementacji i wycofania systemów teleinformatycznych.
- Procedura zarządzania dostępem do sieci i systemów.
- Procedura zarządzania i konfiguracji hardware/software.
- Procedura organizacji środków ochrony fizycznej.
- Procedura współpracy z dostawcami w zakresie bezpieczeństwa informacji.

Warunki realizacji zamówienia:

Opracowanie dokumentacji SZBI w formacie edytowalnym (.docx) oraz PDF.

Etap II. Audyt końcowy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Audyt końcowy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz zgodności z Krajowymi Ramami Interoperacyjności (KRI) i ustawą o krajowym systemie cyberbezpieczeństwa (uoKSC) dla Urzędu Gminy Susiec w ramach realizacji projektu „Cyberbezpieczny Samorząd”.

Zakres audytu:

Audyt obejmuje kompleksową ocenę zgodności aktualnie wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z wymaganiami:

- Normy PN-EN ISO/IEC 27001:2023-08
- Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077 z późn. zm. – uoKSC),
- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773 – KRI),

2. Szczegółowy zakres audytu

- a. Weryfikacja dokumentacji SZBI
 - Ocena kompletności i aktualności dokumentacji SZBI, w tym polityki bezpieczeństwa informacji, procedur zarządzania ryzykiem, zarządzania incydentami, ciągłości działania, zarządzania zasobami informatycznymi oraz zarządzania uprawnieniami.
 - Analiza zgodności dokumentacji z cyklem PDCA (Plan-Do-Check-Act) oraz z aktualnymi wymaganiami normatywnymi i prawnymi.
- b. Audyt organizacyjny
 - Weryfikacja regulacji wewnętrznych w obszarze zarządzania bezpieczeństwem informacji oraz procedur ich audytów i aktualizacji.
 - Ocena zasad postępowania z informacjami, procedur zgłaszania incydentów, zasad reagowania na podatności systemów teleinformatycznych, zasad dostępu do systemów operacyjnych oraz procedur audytu wewnętrznego i aktualizacji dokumentacji.
 - Weryfikacja odpowiedzialności i uprawnień pracowników, procedur zmiany uprawnień, analizy dokumentacji dotyczącej bezpieczeństwa informacji w kontekście umów wykonawczych i serwisowych, analizy ryzyka oraz polityki zapewnienia ciągłości działania.
- c. Audyt fizyczny i środowiskowy
 - Weryfikacja granic obszaru bezpiecznego, zabezpieczeń wejścia/wyjścia, procedur zarządzania bezpieczeństwem fizycznym oraz procedur zapewnienia ciągłości działania i zabezpieczeń infrastruktury fizycznej.
- d. Audyt teleinformatyczny
 - Weryfikacja stosowania procedur zarządzania, konfiguracji i zabezpieczeń systemów teleinformatycznych.
 - Przegląd zasobów informatycznych oraz rozwiązań dla zapewnienia ciągłości działania, minimalizowania ryzyka utraty informacji, ochrony przed błędami, utratą, ujawnieniem, nieuprawnioną modyfikacją danych, bezpieczeństwa sieci wewnętrznej, komputerów, urządzeń mobilnych oraz metod zapobiegania nieautoryzowanym operacjom.
 - Stosowanie mechanizmów kryptograficznych, zabezpieczeń antywirusowych, zabezpieczeń przed nieautoryzowanym dostępem, systemów monitorowania i

reagowania na incydenty, zarządzania aktualizacjami oprogramowania, zabezpieczeń stacji roboczych i nośników danych, stosowania polityki haseł, fizycznych zabezpieczeń urządzeń oraz pomieszczeń.

e. Analiza zgodności z KRI

- Weryfikacja zgodności polityki bezpieczeństwa informacji z KRI, procedur zmiany uprawnień, zgodności procedur zarządzania IT z minimalnymi wymaganiami KRI.

3. Wymagania formalne

- Audyt musi być przeprowadzony przez co najmniej jednego audytora który posiada certyfikat uprawniający do przeprowadzenia audytu według wymagań ustawy o krajowym systemie cyberbezpieczeństwa.
- Wykonawca zobowiązany jest do przedstawienia dokumentów potwierdzających, że audytorzy przeprowadzający audyt posiadają przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999), w szczególności:
 - ✓ Certified Internal Auditor (CIA),
 - ✓ Certified Information System Auditor (CISA),
 - ✓ Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001:2023-08 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób,
 - ✓ Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
 - ✓ Certified Information Security Manager (CISM),
 - ✓ Certified in Risk and Information Systems Control (CRISC),
 - ✓ Certified in the Governance of Enterprise IT (CGEIT),
 - ✓ Certified Information Systems Security Professional (CISSP),
 - ✓ Systems Security Certified Practitioner (SSCP),
 - ✓ Certified Reliability Professional,
 - ✓ Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Zamawiający zastrzega możliwość weryfikacji ważności uprawnień audytorów oraz akredytacji jednostki wydającej certyfikaty.

Audytorzy muszą być niezależni od zespołu wdrażającego SZBI.

Etap III. Raport końcowy

Na podstawie przeprowadzonego audytu Wykonawca opracuje raport końcowy zawierający:

- Wprowadzenie (cel, zakres, jednostki objęte audytem, metodyka),
- Oceny zgodności z normami i przepisami,
- Identyfikację niezgodności oraz słabości systemu,
- Opis mocnych stron i dobrych praktyk,
- Rekomendacje i zalecenia naprawcze oraz propozycje działań doskonalących,
- Propozycję priorytetów i terminów realizacji działań naprawczych,
- Sugerowane terminy przyszłych audytów lub działań kontrolnych,
- Podpisy i oświadczenie audytorów,

- Załączniki (lista dokumentów, sprzętu, konfiguracji sieci, protokoły wywiadów).

Audyt końcowy ma na celu potwierdzenie poprawy poziomu cyberbezpieczeństwa w jednostkach oraz osiągnięcia celów projektu grantowego „Cyberbezpieczny Samorząd”.

