



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Załącznik nr 1
do Zapytania ofertowego nr WP.042.4.3.2025.AM

OPIS PRZEDMIOTU ZAMÓWIENIA

na opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, przeprowadzenie szkoleń oraz wykonanie audytu dla Starostwa Powiatowego w Szczecinku, Domu Pomocy Społecznej w Bornem Sulinowie i Zespołu Szkół Nr 7 w Białym Borze, w ramach projektu grantowego „Cyberbezpieczny samorząd” Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Przedmiotem zamówienia jest przegląd, opracowanie i dostosowanie do nowych wymagań prawnych oraz wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, przeprowadzenie szkoleń oraz wykonanie audytu i Ankiety Dojrzałości Cyberbezpieczeństwa w JST na zakończenie projektu dla trzech jednostek organizacyjnych Powiatu Szczecineckiego:

- Starostwo Powiatowe w Szczecinku, ul. Warcisława IV 16, 78-400 Szczecinek;
- Dom Pomocy Społecznej w Bornem Sulinowie, ul. Szpitalna 5, 78-449 Borne Sulinowo;
- Zespół Szkół Nr 7 w Białym Borze, ul. Brzeźnicka 10, 78-425 Biały Bór.

Przedmiot zamówienia podzielony został na 2 części:

Część 1: Przegląd istniejących procedur, opracowanie i dostosowanie do nowych wymagań prawnych, wdrożenie dokumentacji SZBI odrębnie dla trzech jednostek organizacyjnych Powiatu Szczecineckiego:

- **Starostwa Powiatowego w Szczecinku;**
- **Domu Pomocy Społecznej w Bornem Sulinowie;**
- **Zespołu Szkół nr 7 w Białym Borze**

oraz przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa.

Dokumentacja SZBI

1. Wymaga się, aby dokumentacja dotycząca SZBI była oparta na już istniejącej i obowiązującej dokumentacji w Starostwie Powiatowym w Szczecinku. Powinna ona zachować tą samą formę oraz zawierać te same dane, z zastrzeżeniem, że wszystkie informacje muszą być zaktualizowane zgodnie z obowiązującymi normami i przepisami, a w przypadku dokumentacji dla Domu Pomocy Społecznej w Bornem Sulinowie oraz Zespołu Szkół nr 7 w Białym Borze dostosowana do regulaminu organizacyjnego tych jednostek oraz funkcjonującego systemu teleinformatycznego.



2. Projekt dokumentacji wymaga konsultacji i uzgodnienia z sekretarzem powiatu, administratorem systemu informatycznego, inspektorem ochrony danych oraz dyrektorami ww. jednostek organizacyjnych.
3. Zamawiający wymaga wykonania usługi zgodnie z wymaganiami bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych oraz aktualnie obowiązującymi normami PN-EN ISO 27001 oraz PN-EN ISO 22301.
4. Zamawiający wymaga, aby dokumentacja dla każdej z jednostek w swoim zakresie obejmowała przynajmniej:

„ I. Postanowienia ogólne (w tym cel wdrożenia SZBI oraz podstawowe definicje),

II. Politykę ochrony danych osobowych, która zawiera minimum :

1. wstęp (co zawiera, w jakim celu polityka została sporządzona);
2. dane administratora danych osobowych (kto pełni funkcje, jakie są jego zadania);
3. kierownicy komórek organizacyjnych (jako odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych w podległych komórkach organizacyjnych, zasady przeglądu systemów w podległych komórkach organizacyjnych, zadania kierowników komórek organizacyjnych);
4. informacje o administratorze systemu informatycznego (zadania i obowiązki);
5. informacje o inspektorze ochrony danych (zadania i obowiązki, w tym w zakresie zgłaszania i obsługi incydentów);
6. zasady przetwarzania danych osobowych;
7. zasady legalności przetwarzania danych;
8. zasady realizacji obowiązku informacyjnego (w tym cykl życia dokumentów i okres ich przechowywania);
9. zasady obsługi praw osób, których dane są przetwarzane;
10. zasady rejestrowania czynności przetwarzania danych osobowych;
11. zasady powierzania przetwarzania danych podmiotom zewnętrznym;
12. środki techniczne i organizacyjne służące zapewnieniu integralności, poufności i rozliczalności;
13. zasady szkoleń w tym odpowiedzialność kierowników komórek organizacyjnych;
14. upoważnienia do przetwarzania danych osobowych– zasady nadawania, cofania, wzory;
15. zasady monitorowania przestrzegania zasad ochrony danych osobowych;
16. opracowane załączniki do polityki ochrony danych osobowych minimum:
 - załącznik nr 1 – Procedura obsługi żądań osób, których dane dotyczą.
 - załącznik nr 2 – Zgłoszenie czynności przetwarzania danych osobowych do Rejestru czynności przetwarzania danych osobowych
 - załącznik nr 3 – Zgłoszenie kategorii powierzonych przetwarzania danych osobowych do Rejestru kategorii czynności przetwarzania Danych Osobowych
 - załącznik nr 4 – Ankieta oceny bezpieczeństwa przetwarzania danych osobowych przez podmiot przetwarzający
 - załącznik nr 5 – Regulamin ochrony danych osobowych (w tym: obowiązek zachowania poufności i ochrony danych osobowych, zasady bezpiecznego użytkowania sprzętu



informatycznego, zasady pracy w systemach informatycznych, polityka haseł, zasady korzystania z internetu, zasady korzystania z poczty elektronicznej, ochrona antywirusowa, zasady bezpiecznego korzystania z komputerów przenośnych, zabezpieczenie dokumentacji papierowej z danymi osobowymi, postępowanie dyscyplinarne,

- załącznik nr 6 – Oświadczenie o zachowaniu poufności*
- załącznik nr 7 – Raport z naruszenia ochrony danych osobowych.*

III. Instrukcję zarządzania systemem informatycznym

- 1. zasady ogólne;*
- 2. procedury nadawania, zmiany i odbierania uprawnień do przetwarzania danych osobowych w systemach Informatycznych;*
- 3. metody i środki uwierzytelniania;*
- 4. zarządzanie uprawnieniami administratorów;*
- 5. procedura tworzenia kopii zapasowych;*
- 6. zabezpieczenie systemu informatycznego;*
- 7. wykonywanie przeglądów i konserwacji systemu;*
- 8. likwidacja nośników danych.*

IV. Zarządzanie i zasady postępowania z incydentami bezpieczeństwa

V. Zasady bezpiecznej pracy zdalnej

- 1. Miejsce świadczenia pracy zdalnej;*
- 2. Internet;*
- 3. Urządzenia służące do pracy zdalnej;*
- 4. Zabezpieczanie przekazywanych informacji;*
- 5. Zasady korzystania z dokumentów;*
- 6. Zasady bezpiecznego prowadzenia wideokonferencji;*
- 7. Działania niedozwolone.*

VI. Zasady zarządzania ciągłością działania

- 1. Zasady ogólne;*
- 2. Zapewnienie ciągłości pracy systemu z udziałem systemów informatycznych;*
- 3. Zapewnienie ciągłości pracy bez udziału systemów informatycznych.*

VII. Bezpieczeństwo fizyczne i środowiskowe

- 1. Bezpieczeństwo fizyczne;*
- 2. Bezpieczeństwo środowiskowe.*

VIII. Postępowanie i zarządzanie ryzykiem

IX. Załącznik do SZBI - oświadczenie o zapoznaniu się z treścią dokumentów składających się na system zarządzania bezpieczeństwem informacji”.

Zakres zamówienia obejmuje:

1. Przegląd istniejących procedur SZBI i innych procedur wewnętrznych pod kątem zgodności z obowiązującymi przepisami i normami, istotności w kontekście docelowego SZBI oraz określenia brakującej dokumentacji.
2. Opracowanie nowej/poprawionej dokumentacji SZBI na wzorze istniejącej;
3. Doradztwo w ustanowieniu i wdrożeniu SZBI, w tym:



- Omówienie obowiązków wynikających z SZBI,
 - Wskazanie działań, jakie musi podjąć Zamawiający w celu wdrożenia SZBI,
 - Wskazanie niezbędnego zakresu uzupełnienia dokumentacji przez Zamawiającego,
 - Weryfikacja dokumentacji uzupełnionej przez Zamawiającego,
 - Instruktaż z szacowania ryzyka,
 - Weryfikację szacowania ryzyka przeprowadzonego przez Zamawiającego,
 - Instruktaż z inwentaryzacji aktywów informacyjnych,
 - Weryfikację wyników inwentaryzacji przeprowadzonej przez Zamawiającego,
 - Instruktaż z opracowania upoważnień do przetwarzania informacji
 - Weryfikację upoważnień do przetwarzania informacji opracowanych przez Zamawiającego.
4. Udział w audycie SZBI, który zostanie zamówiony w ramach części 2 zamówienia i przeprowadzony przez innego wykonawcę w terminie określonym w umowie. Realizacja tego punktu stanowić będzie zobowiązanie gwarancyjne Wykonawcy i nie będzie stanowiła podstawy do żądania dodatkowego wynagrodzenia. Jeśli audyt SZBI ujawni nieprawidłowości lub braki wynikające z winy Wykonawcy, będzie on zobowiązany do dostosowania dokumentacji do zaleceń po audytowych.
5. Produktem realizacji części 1 zamówienia ma być kompletna dokumentacja SZBI odrębnie dla każdej z trzech jednostek organizacyjnych Powiatu Szczecineckiego, a mianowicie:
- Starostwa Powiatowego w Szczecinku
 - Domu Pomocy Społecznej w Bornem Sulinowie
 - Zespołu Szkół nr 7 w Białym Borze.
6. Dokumentacja SZBI będzie wykonana w oparciu o:
- wymagania wynikające z 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;
 - wymagania wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
 - wymagania wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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);
 - wymagania wynikające z Dyrektywy 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 uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2);
 - aktualne normy PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 27701, oraz PN-ISO/IEC 22301



7. Ponadto Wykonawca zobowiązany jest uwzględnić Narodowe Standardy Cyberbezpieczeństwa, będące zbiorem rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych.
8. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa *o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* bądź inne przepisy implementujące Dyrektywę 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 uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) do polskiego systemu prawnego Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem.
9. Projekty poszczególnych elementów składowych dokumentacji SZBI będą przedstawiane Zamawiającemu do akceptacji. Zamawiający dopuszcza przesyłanie roboczych dokumentów projektowych drogą elektroniczną. Odbiorowi podlegać będą tylko uprzednio zaakceptowane projekty dokumentów.
10. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przedstawianych projektów dokumentacji SZBI, w tym do rodzaju dokumentów, ich liczby, nazewnictwa, zakresu merytorycznego. Uwagi Zamawiającego powinny być każdorazowo uwzględniane przez Wykonawcę. W przypadku gdy Wykonawca uzna, iż proponowane przez Zamawiającego zmiany będą powodowały niezgodność dokumentacji z Umową poinformuje o tym Zamawiającego, uzasadniając swoje stanowisko. W takiej sytuacji Zamawiający podejmie ostateczną decyzję w sprawie uwzględnienia swoich uwag.
11. Dokumenty będą zawierać wyłącznie autorskie treści powstałe w wyniku realizacji zamówienia oraz inne autorskie treści Wykonawcy, które nie są publicznie dostępne. Będą opracowaniem kompletnym i wyczerpującym z punktu widzenia celu, któremu mają służyć.

Wykonawca będzie zobligowany, do przeprowadzenia minimum 3 spotkań stacjonarnych z kierownikami komórek organizacyjnych Starostwa oraz dyrektorami jednostek organizacyjnych, w celu dokonania analizy i identyfikacji procedur i procesów na potrzeby opracowywanej dokumentacji.

Szkolenia

W ramach zamówienia Wykonawca przeprowadzi stacjonarne szkolenia z zakresu cyberbezpieczeństwa dla 155 pracowników Starostwa Powiatowego w Szczecinku, Domu Pomocy Społecznej w Bornem Sulinowie i Zespołu Szkół Nr 7 w Białym Borze.

Celem szkoleń jest podniesienie poziomu wiedzy i kompetencji kadry JST z zakresu cyberbezpieczeństwa, przede wszystkim z punktu widzenia SZBI wdrażanej w ramach części I zamówienia i ról, które poszczególne osoby pełnią w ramach SZBI.

Nacisk ma zostać położony na podniesienie świadomości zagrożeń i reakcji osób posiadających wyznaczone obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami, umiejętność oceny sytuacji naruszenia cyberbezpieczeństwa, identyfikację prób ataków (w tym ataków

socjotechnicznych) i podejmowania odpowiednich kroków w celu ich zneutralizowania oraz na podejmowane działania i postępowanie zgodnie z procedurami i rolami w SZBI. Szkolenie ma być zorientowane na praktyczne wykorzystanie wiedzy zdobytej podczas kursu.

Szkolenia podzielone będą na 3 zakresy:

Szkolenie kadry nietechnicznej w zakresie cyberbezpieczeństwa – szkolenie podstawowe – Security Awareness

Liczba uczestników szkolenia – 120 osób

Liczba grup szkoleniowych – minimum 3 po 40 osób

Czas trwania szkolenia dla jednej grupy – minimum 3,5 godziny, w tym dwie przerwy po 15 minut każda. Po zakończeniu szkolenia, przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

Szkolenie odbywać się będzie od poniedziałku do piątku w godzinach 8:00 – 15:00, stacjonarnie w siedzibie Starostwa Powiatowego w Szczecinku

Szkolenie stacjonarne z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

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

Zaawansowane szkolenie z zakresu cyberbezpieczeństwa dla kadry zarządzającej – szkolenie rozszerzone – Security Awareness

Liczba uczestników szkolenia – 34 osoby

Czas trwania szkolenia – minimum 3,5 godziny, w tym dwie przerwy po 15 minut każda. Po zakończeniu szkolenia, przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

Szkolenie odbywać się będzie od poniedziałku do piątku w godzinach 8:00 – 15:00, stacjonarnie w siedzibie Starostwa Powiatowego w Szczecinku



Celem szkolenia jest przekazanie dla kadry kierowniczej jednostki, wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

Zakres tematyki szkolenia musi obejmować co najmniej:

1. Podstawowe zasady i regulacje z zakresu cyberbezpieczeństwa:
 - przegląd aktualnych regulacji prawnych (RODO, NIS2, ISO 27001),
 - wymagania i standardy dotyczące zarządzania bezpieczeństwem informacji,
 - identyfikacja i ocena ryzyk cybernetycznych,
 - techniki oceny ryzyka i analizy zagrożeń.
2. Nowoczesne zagrożenia cybernetyczne i sposoby obrony:
 - najnowsze techniki ataków (phishing, ransomware, APT),
 - wykorzystanie zaawansowanych narzędzi ochrony,
 - rola kadry zarządzającej w tworzeniu kultury bezpieczeństwa,
 - strategia komunikacji wewnętrznej i edukacji pracowników.
3. Wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):
 - zasady i korzyści wynikające z wdrożenia SZBI,
 - przegląd normy ISO 27001, w tym kluczowe wymagania, polityki oraz struktury systemu zarządzania,
 - rola kadry zarządzającej w kontekście SZBI,
 - obowiązki i odpowiedzialność kierownictwa w ramach SZBI,
 - Monitorowanie, przegląd i doskonalenie SZBI, w tym planowanie i wdrażanie działań doskonalących.

Szkolenie kadry technicznej IT z zakresu cyberbezpieczeństwa

Liczna uczestników szkolenia – 1 osoba

Liczba godzin szkoleniowych – szkolenie musi trwać co najmniej 2 dni szkoleniowe. Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min.).

Szkolenie odbywać się będzie od poniedziałku do piątku w godzinach 8:00 – 15:00, stacjonarnie w siedzibie Starostwa Powiatowego w Szczecinku

Zakres tematyki szkolenia, musi obejmować co najmniej:

Moduł 1: Podstawy cyberbezpieczeństwa

1. Wprowadzenie do cyberbezpieczeństwa: definicja, znaczenie i aktualne zagrożenia.
2. Rodzaje ataków cybernetycznych: malware, phishing, ransomware, ataki DDoS itp.
3. Podstawowe pojęcia związane z cyberbezpieczeństwem: poufność, integralność, dostępność, poufność, niezaprzeczalność.
4. Regulatory i standardy związane z cyberbezpieczeństwem: GDPR, ISO 27001.

Moduł 2: Bezpieczeństwo sieci

1. Zagrożenia związane z sieciami komputerowymi.
2. Architektura sieciowa i zasady projektowania bezpiecznej sieci.



3. Firewallle: rodzaje, konfiguracja i zarządzanie nimi.
4. Zabezpieczanie sieci bezprzewodowych: uwierzytelnianie, szyfrowanie, filtrowanie adresów MAC.
5. Zarządzanie hasłami i autoryzacją: zasady tworzenia silnych haseł, zarządzanie kontami użytkowników.

Moduł 3: Bezpieczeństwo systemów operacyjnych

1. Aktualizacje systemów operacyjnych i aplikacji: znaczenie i procedury.
2. Antywirusy i antimalware: instalacja, konfiguracja i skanowanie systemu.
3. Bezpieczne korzystanie z systemu: zasady tworzenia kont użytkowników, zarządzanie uprawnieniami.
4. Monitorowanie systemu: logi, analiza zdarzeń bezpieczeństwa, wykrywanie nieprawidłowości.

Moduł 4: Bezpieczeństwo aplikacji

1. Testowanie penetracyjne: zasady, narzędzia i techniki.
2. Ochrona przed atakami typu SQL injection i cross-site scripting.
3. Bezpieczeństwo aplikacji webowych: filtrowanie wejścia, zabezpieczanie sesji, walidacja danych.

Moduł 5: Zarządzanie incydentami i reagowanie na ataki

1. Planowanie reakcji na incydenty: tworzenie procedur, zespoły odpowiedzialne za reagowanie.
2. Analiza zdarzeń bezpieczeństwa: narzędzia i techniki identyfikacji i analizy ataków.
3. Reagowanie na incydenty: odizolowanie systemów, odzyskiwanie danych, przywracanie działania.
4. Audyt bezpieczeństwa: przegląd systemów, ocena zgodności z zasadami bezpieczeństwa.

Moduł 6: Polityka bezpieczeństwa i świadomość użytkowników

1. Tworzenie polityki bezpieczeństwa: cele, zasady i procedury.
2. Szkolenia dla pracowników: edukacja w zakresie bezpiecznego korzystania z technologii.
3. Zarządzanie ryzykiem: ocena ryzyka, zarządzanie incydentami, planowanie ciągłości działania.
4. Bezpieczeństwo w chmurze: zagrożenia i najlepsze praktyki związane z usługami chmurowymi.

Program szkolenia będzie obejmował zarówno wykłady teoretyczne, jak i praktyczne warsztaty, w których uczestnik będzie mógł zastosować zdobytą wiedzę w praktyce. Podczas szkolenia będą używane różne narzędzia i symulacje, aby umożliwić uczestnikowi eksplorację rzeczywistych scenariuszy i sytuacji związanych z cyberbezpieczeństwem.

Do każdego z powyższych punktów muszą zostać przygotowane laboratoria, podczas których należy przedstawić praktyczne metody ochrony przed konkretnym atakiem.

Wykonawca zobowiązany będzie przedstawić do każdego szkolenia osobno:



1. Program szkolenia, oznaczony zgodnie z zasadami określonymi w „Podręczniku wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji”.
2. Kadre trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia.
3. Materiały szkoleniowe, przygotowane w wersji papierowej i elektronicznej, zgodnie ze standardem cyfrowym, oznaczone zgodnie z zasadami określonymi w „Podręczniku wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji”.
4. Listy obecności podpisane przez uczestników szkoleń, oznaczone zgodnie z zasadami określonymi w „Podręczniku wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji”.
5. Certyfikat uczestnictwa dla każdego uczestnika szkolenia, podpisany przez trenera i ukończenie szkolenia i jego zakres, oznaczony zgodnie z zasadami określonymi w „Podręczniku wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji”.

Szkolenie musi być zakończone anonimową ankietą wśród uczestników, oceniającą co najmniej przydatność szkolenia, zakres przekazanych informacji, adekwatność przekazanych informacji do potrzeb uczestników, formę prezentacji i komunikatywność prowadzącego szkolenie. Wykonawca przedstawi Zamawiającemu podsumowanie wyników ankiety.

Część 2: Wykonanie audytu SZBI, zgodności z wymaganiami Rozporządzenia KRI i ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz przeprowadzenie Ankiety Dojrzałości Cyberbezpieczeństwa w JST na zakończenie projektu, dla trzech jednostek organizacyjnych Powiatu Szczecineckiego:

- **Starostwa Powiatowego w Szczecinku;**
- **Domu Pomocy Społecznej w Bornem Sulinowie;**
- **Zespołu Szkół nr 7 w Białym Borze.**

W ramach realizacji części 2 zamówienia Wykonawca zobowiązany będzie do wykonania dwóch audytów odrębnie dla trzech jednostek organizacyjnych Powiatu Szczecineckiego:

1. audytu zaktualizowanego SZBI, który będzie wykonany w ramach części 1 zamówienia, pod względem zgodności systemu z wymogami prawnymi i normami, a w szczególności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077 z późn. zm.),
2. audytu zgodności z rozporządzeniem 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. 2024 poz. 773) oraz z technicznymi wymaganiami wynikającymi z uoKSC, potwierdzającego zrealizowanie grantu na koniec projektu.



1. Audyt zaktualizowanego SZBI

Przeprowadzenie audytu SZBI musi pozwolić na weryfikację poprawności stosowanych procedur i zabezpieczeń w odniesieniu do założonych wymagań. Audyt zgodności z KRI ma potwierdzić czy w wyniku realizacji projektu grantowego podniesiony został poziom cyberbezpieczeństwa w jednostkach i czy osiągnięte zostały cele projektu. W wyniku obu audytów mają zostać przygotowane raporty podsumowujące przeprowadzone weryfikacje, zawierające omówienie wszystkich niezgodności.

Audyt powinien mieć charakter proceduralny, a jego zakres musi uwzględniać wytyczne normy ISO 27001 oraz specyficzne wymagania proceduralne uoKSC, ze szczególnym naciskiem na obowiązki związane z cyberbezpieczeństwem, zarządzaniem ryzykiem oraz reakcją na incydenty.

Zakres audytu:

Audyt organizacyjny obejmujący:

1. Weryfikację regulacji wewnętrznych Zamawiającego w obszarze zarządzania bezpieczeństwem informacji oraz procedur ich audytów i aktualizacji, w tym zgodności z normą ISO 27001 oraz z uoKSC:
 - Zasady postępowania z informacjami, w szczególności zapewniające minimalizację ryzyka kradzieży informacji, nieuprawnionego dostępu, uszkodzeń, zakłóceń oraz kradzieży środków przetwarzania informacji, w tym urządzeń mobilnych.
 - Procedury zgłaszania incydentów bezpieczeństwa, uwzględniające obowiązek raportowania incydentów do odpowiednich zespołów CSIRT, w tym określenie reakcji na różne typy zagrożeń.
 - Zasady reagowania na podatności systemów teleinformatycznych: analiza procedur działania w przypadku wykrycia lub publikacji informacji o podatnościach technicznych systemów oraz w zakresie współpracy z podmiotami odpowiedzialnymi za cyberbezpieczeństwo.
 - Zasady dostępu do systemów operacyjnych: weryfikacja polityk kontroli dostępu oraz zabezpieczeń przed nieautoryzowanymi instalacjami oprogramowania.
 - Procedury audytu wewnętrznego i aktualizacji dokumentacji.
3. Weryfikację odpowiedzialności i uprawnień pracowników w zakresie zarządzania bezpieczeństwem informacji, w tym danych osobowych, zgodnie z wymaganiami SZBI oraz uoKSC, z uwzględnieniem odpowiednich szkoleń oraz certyfikacji.
4. Weryfikację procedur zmiany uprawnień w przypadku rotacji kadr i/lub zmiany zadań pracowników, zgodnie z wymogami SZBI oraz uoKSC, obejmującą procedury nadawania, modyfikowania i odbierania dostępu do informacji wrażliwych.
5. Analizę dokumentacji dotyczącej bezpieczeństwa informacji w kontekście zawierania umów wykonawczych i serwisowych, zgodnie z wymaganiami SZBI oraz uoKSC, z uwzględnieniem odpowiednich klauzul ochrony danych i odpowiedzialności stron trzecich za naruszenia bezpieczeństwa.



6. Analizę ryzyka: weryfikację procedur analizy ryzyka utraty integralności, dostępności i poufności informacji zgodnie z wymogami SZBI oraz uoKSC, w tym ocenę mechanizmów aktualizacji tej analizy oraz stosowania odpowiednich środków zaradczych.
7. Weryfikację polityki zapewnienia ciągłości działania i planów awaryjnych.

Audyt fizyczny i środowiskowy

Audyt fizyczny i środowiskowy należy przeprowadzić we wszystkich trzech lokalizacjach Starostwa Powiatowego w Szczecinku. Audyt obejmuje:

1. Weryfikację granic obszaru bezpiecznego, obejmującą fizyczne granice miejsc, gdzie przetwarzane są informacje wrażliwe, oraz dostępność i funkcjonalność zabezpieczeń fizycznych.
2. Zabezpieczenia wejścia/wyjścia: procedury kontroli dostępu do pomieszczeń (np. serwerowni i archiwów) i autoryzacji.
3. Procedury zarządzania bezpieczeństwem fizycznym, w tym monitorowania dostępu i ochrony przed zagrożeniami fizycznymi.
4. Procedury zapewnienia ciągłości działania i zabezpieczeń infrastruktury fizycznej, w tym wymagania w zakresie zasilania awaryjnego, procedury zarządzania awariami, itp.

2. Audyt zgodności z KRI

Audyt powinien mieć charakter proceduralny, a jego zakres musi uwzględniać specyficzne wymagania KRI i techniczne wymagania wynikające z uoKSC oraz koncentrować się na zabezpieczeniach infrastruktury IT, systemach teleinformatycznych, bezpieczeństwie sieci i systemów. Zakres audytu:

Audyt organizacyjny obejmujący:

1. Weryfikację zgodności polityki bezpieczeństwa informacji z KRI, w tym:
 - Zasady bezpiecznej pracy mobilnej i pracy zdalnej, uwzględniające środki techniczne i organizacyjne chroniące przed zagrożeniami wynikającymi z pracy na odległość, w tym politykę haseł oraz ochronę połączeń zdalnych.
2. Weryfikację stosowania procedur zmiany uprawnień w przypadku rotacji kadi i/lub zmiany zadań pracowników, obejmującą procedury nadawania, modyfikowania i odbierania dostępu do informacji wrażliwych.
3. Weryfikację zgodności procedur zarządzania IT z minimalnymi wymaganiami KRI.

Audyt teleinformatyczny:

Audyt teleinformatyczny należy przeprowadzić we wszystkich trzech jednostkach organizacyjnych. Audyt obejmuje:

1. Weryfikację stosowania procedur zarządzania, konfiguracji i zabezpieczeń systemów teleinformatycznych: zgodność KRI w zakresie zarządzania bezpieczeństwem systemów, w tym aktualizacji, monitorowania i reagowania na incydenty.
2. Przegląd zasobów informatycznych oraz rozwiązań dla zapewnienia ciągłości działania:



- Minimalizowanie ryzyka utraty informacji w wyniku awarii: analiza kopii zapasowych i procedur ich testowania, redundancji zasobów, systemów podtrzymania zasilania, chłodzenia oraz alarmów i przywracania działania systemów po incydencie.
 - Ochrona przed błędami, utratą, ujawnieniem, nieuprawnioną modyfikacją danych, bezpieczeństwo sieci wewnętrznej, komputerów, urządzeń mobilnych oraz metod zapobiegania nieautoryzowanym operacjom: zgodność z KRI. Stosowanie mechanizmów kryptograficznych: ocena wdrożonych rozwiązań kryptograficznych zgodnych z uoKSC i KRI.
 - Bezpieczeństwo plików systemowych: weryfikacja zgodności z wymogami zabezpieczeń systemowych.
 - Weryfikacja zabezpieczeń antywirusowych.
 - Weryfikacja zabezpieczeń przed nieautoryzowanym dostępem, w tym urządzeń firewall i/lub UTM.
 - Weryfikacja systemów monitorowania i reagowania na incydenty (SIEM, IDS/IPS) i/lub usług centrów monitorowania bezpieczeństwa (SOC).
3. Zarządzanie aktualizacjami oprogramowania: weryfikację procedur zarządzania aktualizacjami oprogramowania, zgodnie z KRI, w tym automatyzacji i monitorowania procesu aktualizacji.
 4. Zabezpieczenia stacji roboczych i nośników danych: weryfikację bezpieczeństwa stacji roboczych i nośników danych, w tym ich szyfrowania i fizycznej ochrony, zgodnie z uoKSC i KRI.
 5. Weryfikację stosowania polityki haseł: zgodność stosowanych polityk tworzenia, przechowywania i zmiany haseł z wymogami KRI i uoKSC, w tym zabezpieczeń przed nieautoryzowanym dostępem.
 6. Weryfikację fizycznych zabezpieczeń urządzeń oraz pomieszczeń, w tym dostępności systemów monitoringu i alarmowych.
 7. Audytowi podlega całość sprzętu informatycznego będącego w posiadaniu Zamawiającego (w tym sprzęt nabywany w ramach grantu).

Dokumentacja po zakończeniu audytów

Po zakończeniu każdego z audytów Wykonawca przygotowuje raport zawierający wnioski dotyczące stanu obecnego, wytyczne do dalszego doskonalenia i rekomendacje w zakresie poprawy cyberbezpieczeństwa na przyszłość. Dokumentacje poaudytowe muszą obejmować co najmniej:

- Wprowadzenie (cel audytu, zakres, kluczowe obszary audytowane, datę przeprowadzenia audytu, opis jednostek, systemów, procedur i obszarów objętych audytem);
- Opis zastosowanych metod i działań audytowych;
- Ocenę zgodności z przepisami: Ogólna ocena stopnia zgodności odpowiednio z uoKSC, KRI oraz innymi regulacjami i normami, takimi jak RODO lub ISO 27001;
- Identyfikację niezgodności: Wyszczególnienie obszarów, w których audyt wykazał brak zgodności z wymaganiami prawnymi lub procedurami wewnętrznymi. Każda



niezgodność powinna być opisana i sklasyfikowana (np. krytyczna, wysoka, średnia, niska),

– Wyniki audytu, w tym:

- opis mocnych stron – obszarów, w których jednostki spełniają wymogi i wykazują się dobrymi praktykami w zakresie zarządzania bezpieczeństwem informacji;
- wskazanie słabych punktów – wykrytych podatności, niezgodności lub braków w procedurach oraz zabezpieczeniach technicznych i organizacyjnych;
- ocenę ryzyka – analizę wykrytych ryzyk związanych z bezpieczeństwem informacji, obejmującą ryzyka dla integralności, poufności i dostępności danych oraz systemów;

– Rekomendacje i zalecenia audytorów zawierające:

- zalecane działania naprawcze (np. wzmocnienie polityk bezpieczeństwa, poprawę lub wprowadzenie procedur reagowania na incydenty, dostosowanie zabezpieczeń technicznych i organizacyjnych),
- priorytetyzację działań (np. podział działań na krytyczne, pilne, zalecane), aby umożliwić organizacji skuteczne planowanie działań naprawczych,
- propozycję terminów realizacji działań naprawczych
- sugerowane terminy przyszłych audytów lub działań kontrolnych w celu zapewnienia ciągłej zgodności;

– Podpisy i oświadczenia audytorów (np. o rzetelności przeprowadzonego audytu i pełnym przedstawieniu wyników oraz wniosków);

– Załączniki (np. listę uczestników audytu, listę przeanalizowanych dokumentów, polityk i procedur, listę sprzętu, konfigurację sieci).

Forma przekazania i omówienia raportu: Spotkanie w siedzibach jednostek organizacyjnych Zamawiającego, podczas którego wyniki audytu zostaną omówione z kadrą kierowniczą.

Przeprowadzenie Ankiety Dojrzałości Cyberbezpieczeństwa w JST na zakończenie projektu

Wykonawca zobowiązany będzie do przeprowadzenia *Ankiety Dojrzałości Cyberbezpieczeństwa w jednostkach samorządu terytorialnego*, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 9 do zapytania ofertowego. Ankieta obejmuje trzy jednostki organizacyjne Powiatu Szczecineckiego, tj. Starostwo Powiatowe w Szczecinku, Dom Pomocy Społecznej w Bornem Sulinowie i Zespół Szkół Nr 7 w Białym Borze i musi zostać przeprowadzona dla każdej jednostki osobno.

Wymagania ogólne (do dwóch części zamówienia)

1. Wykonawca w ramach wykonania każdej z części zamówienia **przygotuje szczegółowy harmonogram realizacji zamówienia** i przedstawi go Zamawiającemu do akceptacji



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



w terminie nie dłuższym, niż 5 dni roboczych od podpisania umowy na realizację danej części zamówienia.

2. We wszystkich częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. Zapisy SZBI muszą być otwarte, inkluzywne i niedyskryminujące. W przypadku szkolenia stacjonarnego wykonawca będzie musiał zapewnić materiał szkoleniowy z większym rozmiarem czcionki (w zależności od potrzeb uczestników szkolenia). W ramach grup szkoleniowych przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane dokumenty (w tym dokumentacja SZBI, raporty z audytów i materiały szkoleniowe) będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. Zamawiający dopuszcza dostarczenie dokumentacji w formie elektronicznej, np. dokumenty w standardzie PDF.