Przedmiotem zamówienia jest: Opracowanie i wdrożenie Systemu Zarządzaniem Bezpieczeństwem Informacji (zwanego dalej SZBI) w Urzędzie Miejskim (UM) w Chojnowie, w tym również w Urzędzie Stanu Cywilnego (USC) w Chojnowie. Opracowanie i wdrożenie muszą zostać poprzedzone audytem wstępnym, a zakończone muszą być szkoleniem powdrożeniowym i audytem końcowym. Wykonawca przeprowadzi ponadto szkolenie z cyberbezpieczeństwa dla pracowników.

Zamówienie musi być zrealizowane zgodnie z warunkami i wytycznymi konkursu grantowego „Cyberbezpieczny Samorząd", Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).

Minimalne wymagania dot. audytu wstępnego (zerowego):

Podstawa i standardy realizacji audytu: Audyt wstępny musi zostać przeprowadzony w oparciu o aktualny stan prawny i powszechnie uznane standardy międzynarodowe, ze szczególnym uwzględnieniem:

- Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI),
- Ustawy o krajowym systemie cyberbezpieczeństwa (KSC) w zakresie wymagań dla podmiotów ważnych,
- Wytycznych i dobrych praktyk normy PN-EN ISO/IEC 27001,
- Aktualnych przepisów o ochronie danych osobowych, w tym ogólnego rozporządzenia o ochronie danych (RODO).

Minimalny zakres prac:

Etap 1 (Weryfikacja formalno-prawna): Analiza dokumentacji jak np. istniejących zarządzeń, procedur IT, polityk bezpieczeństwa czy dokumentacja ochrony danych osobowych, pod kątem zgodności z KRI.

Etap 2 (Weryfikacja techniczno-fizyczna): Wizja lokalna w siedzibie Zamawiającego obejmująca m.in. wywiady z personelem, ocenę zabezpieczeń fizycznych i środowiskowych oraz weryfikację bezpieczeństwa środowiska IT.

Etap 3 (Analiza luk): Identyfikacja braków pomiędzy stanem faktycznym a wymaganiami prawno-technicznymi oraz inwentaryzacja aktywów niezbędna do późniejszego szacowania ryzyka.

Efektem prac będzie Raport z audytu sporządzony w języku polskim, dostarczony w formie elektronicznej (.PDF), podpisany elektronicznym podpisem kwalifikowanym oraz w formie elektronicznej edytowalnej (np. .DOC / .DOCX).

Raport musi zawierać minimum: Jednoznaczną ocenę stopnia spełnienia wymagań KRI, NIS2 i RODO. Wykaz zidentyfikowanych ryzyk, podatności i luk w zabezpieczeniach. Konkretne wytyczne i rekomendacje techniczno-organizacyjne, które Wykonawca musi bezpośrednio uwzględnić podczas opracowywania dokumentacji SZBI dla Zamawiającego.

Minimalne wymagania dot. opracowywanej dokumentacji SZBI:

1) Deklaracja stosowania zasad i procedur bezpieczeństwa informacji (PBI) – dokument nadrzędny,
2) Pełna dokumentacja Zarządzania Ryzykiem:
- Metodyka zarządzania ryzykiem dopasowana do specyfiki administracji samorządowej,
- Raport z analizy ryzyka (w tym opracowanie/aktualizacja rejestru ryzyk),
- Plany postępowania z ryzykiem.
3) Zasady i procedury operacyjne:
a) Zarządzanie aktywami, ewidencja oraz klasyfikacja informacji,
b) Zapewnienie bezpieczeństwa systemów IT i sieci,
c) Kontrola dostępu i zarządzanie uprawnieniami, w tym zarządzanie dostępem do informacji,
d) Obsługa incydentów bezpieczeństwa, zasady reagowania oraz procedury raportowania do właściwego CSIRT,
e) Polityka kopii zapasowych oraz Plan Odtwarzania Awaryjnego (DRP) systemów krytycznych,
f) Plan Ciągłości Działania (BCP),
g) Bezpieczeństwo pracy zdalnej oraz korzystania z urządzeń mobilnych,
h) Bezpieczeństwo fizyczne i środowiskowe,
i) Bezpieczeństwo zasobów ludzkich,
j) Kryptografia, zasady stosowania metod szyfrowania danych,
k) Bezpieczeństwo łańcucha dostaw,
l) Audyty wewnętrzne, zasady działań korygujących oraz Przeglądy Zarządzania (procedura corocznej oceny SZBI),
m) Komplet szablonów dokumentów operacyjnych niezbędnych do bieżącego prowadzenia systemu.

Dokumentacja musi być opracowana w języku polskim, w sposób zapewniający możliwość jej bezpośredniego wykorzystania do wdrożenia, utrzymania oraz doskonalenia SZBI, zgodnie z uznanymi dobrymi praktykami ISO/IEC 2700x.

Dokumentacja musi zostać dostarczona w formie elektronicznej (.PDF), podpisana elektronicznym podpisem kwalifikowanym oraz w formie elektronicznej edytowalnej (np. .DOC / .DOCX).

Wraz z odbiorem końcowym dokumentacji, Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do wszystkich opracowanych materiałów i dokumentów na wszystkich polach eksploatacji, bez ograniczeń czasowych i terytorialnych, umożliwiając Zamawiającemu ich dowolne kopiowanie, modyfikowanie, aktualizację oraz udostępnianie wewnętrzne.

Przed formalnym zatwierdzeniem dokumentacji Wykonawca zobowiązany jest przeprowadzić spotkanie z kierownictwem. Liczba uczestników: do 8 osób. Czas trwania: min. 1 godzina zegarowa. Minimalny zakres i cele spotkania: Prezentacja wyników analizy ryzyka, wskazanie krytycznych podatności, omówienie ramy odpowiedzialności prawnej kierownictwa (KSC/NIS2) oraz przedstawienie kluczowych założeń przygotowanego projektu SZBI, ostateczne uzgodnienie treści procedur. Wykonawca udzieli ponadto wsparcia przy wydaniu zarządzeń wewnętrznych wprowadzających SZBI.

Minimalne wymagania dot. szkolenia powdrożeniowego:

W ramach wdrożenia Wykonawca zobowiązany jest do przeprowadzenia zamkniętego szkolenia powdrożeniowego dla pracowników UM oraz USC spełniającego następujące wymagania:

Cel szkolenia: Zakomunikowanie personelowi wejścia w życie nowego SZBI oraz omówienie zmian w codziennej pracy urzędu.

Charakter szkolenia: Spotkanie ma mieć charakter zwięzłego instruktażu stanowiskowego i organizacyjnego, bez szczegółowego rozwijania ogólnych tematów z zakresu edukacji o cyberzagrożeniach.

Minimalny zakres tematyczny spotkania: Omówienie celu wdrożenia SZBI w UM i USC (dlaczego te zmiany są wprowadzane, od kiedy obowiązują itp.). Przegląd nowych obowiązków pracowniczych wynikających bezpośrednio z wdrożonych procedur (w tym: zasady czystego biurka/ekranu, zasady zgłaszania awarii i incydentów IT, zasady korzystania ze sprzętu służbowego itp.). Wskazanie osób odpowiedzialnych w strukturze urzędu za nadzór nad SZBI. Przedstawienie i omówienie nowych wzorów dokumentów operacyjnych, które pracownicy będą zobowiązani stosować lub podpisać (np. nowe oświadczenia, wnioski o nadanie/odebranie uprawnień itp.).

Wymagania organizacyjne: Z uwagi na konieczność zachowania ciągłości pracy urzędu i obsługi interesantów w USC, Wykonawca zrealizuje spotkanie w podziale na min. 2 grupy. Liczba osób objętych szkoleniem: do 36, maksymalna liczba osób w jednej grupie: 22. Zamawiający przekaże Wykonawcy listę osób poszczególnych grup biorących udział w szkoleniu do 3 dni roboczych

przed datą rozpoczęcia szkolenia. Czas trwania: min. 1 godzina lekcyjna na grupę. Spotkanie odbyć się musi w siedzibie Zamawiającego, w godzinach pracy Zamawiającego. Zamawiający na czas szkolenia udostępni Wykonawcy salę z dostępem do Internetu, laptopem, rzutnikiem i ekranem. Szkolenie prowadzone będzie w języku polskim. Wykonawca zobowiązany jest do dostarczenia Zamawiającemu podpisanej listy obecności z każdego spotkania oraz do wystawienia imiennych zaświadczeń o wzięciu udziału w szkoleniu powdrożeniowym dla każdego uczestnika.

Minimalne wymagania dot. audytu końcowego (audyt SZBI):

Audyt końcowy (powdrożeniowy) systemu zarządzania bezpieczeństwem informacji musi zostać przeprowadzony w oparciu o aktualny stan prawny i powszechnie uznane standardy międzynarodowe, ze szczególnym uwzględnieniem:

- Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI),
- Ustawy o krajowym systemie cyberbezpieczeństwa (KSC) w zakresie wymagań dla podmiotów ważnych,
- Wytycznych i dobrych praktyk normy PN-EN ISO/IEC 27001,
- Aktualnych przepisów o ochronie danych osobowych, w tym ogólnego rozporządzenia o ochronie danych (RODO),
- Zgodnie z zakresem określonym w Regulaminie Konkursu Grantowego „Cyberbezpieczny Samorząd.

Wykonawca dostarczy Zamawiającemu raport z audytu sporządzony w języku polskim, w formie elektronicznej (.PDF) podpisany elektronicznym podpisem kwalifikowanym oraz w formie elektronicznej edytowalnej (np. .DOC / .DOCX), zawierający minimum opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów.

Wykonawca udzieli wsparcia merytorycznego przy wypełnianiu ankiety dojrzałości cyberbezpieczeństwa (załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”). Wstępnie wypełniona ankieta (stan obecny i planowany) zostanie udostępniona Wykonawcy po podpisaniu umowy.

Minimalne wymagania dot. szkolenia z cyberbezpieczeństwa:

Przedmiotem zamówienia jest przeprowadzenie stacjonarnego szkolenia z zakresu cyberbezpieczeństwa dla pracowników UM i USC z podziałem na grupy.

Cel szkolenia: podniesienie świadomości na temat bezpieczeństwa cyfrowego uczestników wykorzystujących systemy teleinformatyczne w miejscu pracy. Uczestnicy podczas szkolenia będą mogli pogłębić swoją wiedzę oraz nabyć niezbędne umiejętności praktyczne jak przeciwdziałać cyberzagrożeniom.

Wymagania organizacyjne: Z uwagi na konieczność zachowania ciągłości pracy urzędu i obsługi interesantów w USC, Wykonawca zrealizuje spotkanie w podziale na min. 2 grupy. Liczba osób objętych szkoleniem: do 36, maksymalna liczba osób w jednej grupie: 22. Zamawiający przekaże Wykonawcy listę osób poszczególnych grup biorących udział w szkoleniu do 3 dni roboczych przed datą rozpoczęcia szkolenia. Czas trwania: min. 3 godziny lekcyjne na grupę. Spotkanie odbyć się musi w siedzibie Zamawiającego, w godzinach pracy Zamawiającego. Zamawiający na czas szkolenia udostępni Wykonawcy salę z dostępem do Internetu, laptopem, rzutnikiem i ekranem. Szkolenie prowadzone będzie w języku polskim. Wykonawca zobowiązany jest do dostarczenia Zamawiającemu podpisanej listy obecności z każdego spotkania oraz do wystawienia imiennych zaświadczeń o wzięciu udziału w szkoleniu dla każdego uczestnika.

Zamawiający dopuszcza połączenie szkolenia powdrożeniowego SZBI ze szkoleniem z cyberbezpieczeństwa. Czas trwania połączonych szkoleń musi wynosić min. 3 godziny zegarowe na grupę i musi wyczerpywać minimalny zakres tematyczny określony dla obu tych szkoleń. Przeprowadzenie szkolenia dla obu grup jednego dnia jest możliwe tylko wtedy, gdy łączny czas szkolenia obu grup i czas na przerwę pomiędzy grupami nie przekroczą czasu pracy Zamawiającego.

Minimalny zakres tematyczny:

a) wprowadzenie do cyberbezpieczeństwa:

− czym jest cyberbezpieczeństwo;

− dlaczego cyberbezpieczeństwo jest ważne;

− kluczowe zagadnienia związane z cyberbezpieczeństwem;

− przegląd statystyk i trendów w cyberbezpieczeństwie.

b) typy zagrożeń w cyberprzestrzeni:

− malware (wirusy, trojany, robaki itp.);

− ataki typu phishing i spear phishing;
− ataki DDoS;
− ataki ransomware;
− zagrożenia związane z sieciami społecznościowymi;
− cyberprzestępcy a sztuczna inteligencja;
− ataki socjotechniczne;
− przenośne nośniki danych;
c) zasady bezpieczeństwa i praktyki:
− bezpieczne hasła: zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
− zasady bezpieczeństwa e-mail;
− e-Doręczenia, ePUAP, KSeF;
− bezpieczeństwo w sieciach bezprzewodowych;
− bezpieczne przeglądanie internetu;
− backup i odzyskiwanie danych.
d) reagowanie na incydenty i planowanie awaryjne:
− jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
− zasady reagowania na incydenty;
− planowanie awaryjne i kontynuacja działalności;
− przegląd realnych przypadków naruszeń bezpieczeństwa, ich skutki i lekcje z nich wyniesione.

Metody przeprowadzenia szkolenia: szkolenie powinno być prowadzone w formie aktywizującej i integrującej uczestników szkolenia, z wykorzystaniem różnorodnych form, metod i technik dydaktycznych.

Minimalne wymagania dot. Wykonawcy, osób pracujących nad realizacją przedmiotu zamówienia:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą, że w okresie ostatnich 3 lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie), należycie wykonali co najmniej:

- 2 usługi, z których każda polegała na kompleksowym opracowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z Krajowymi Ramami Interoperacyjności (KRI) lub normą ISO/IEC 27001 dla jednostek sektora finansów publicznych, o wartości nie mniejszej niż 15.000,00 zł brutto każda,
- 2 usługi, z których każda polegała na przeprowadzeniu szkolenia z cyberbezpieczeństwa (o tematyce zbliżonej do opisywanej w niniejszym OPZ) dla jednostek sektora finansów publicznych, o wartości nie mniejszej niż 7.500,00 zł brutto każda.

Na potwierdzenie spełnienia powyższych warunków Wykonawca składając ofertę zobowiązany jest przedstawić dowody (np. referencje, protokoły odbioru/końcowe bez zastrzeżeń) i dołączyć wypełniony załącznik nr 6 do zapytania ofertowego – Wykaz usług.

Zamawiający dopuszcza wykazanie wymaganego doświadczenia w ramach usług łączonych (w ramach jednej umowy/zamówienia). W takim przypadku Wykonawca może wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie), należycie wykonał co najmniej minimum 3 kompleksowe usługi łączone, z których każda obejmowała swoim zakresem zarówno opracowanie/wdrożenie SZBI jak i szkolenie z cyberbezpieczeństwa dla min. 20 osób, a łączna wartość brutto każdej pojedynczej usługi łączonej wynosiła nie mniej niż 22.500,00 zł brutto.

Wykonawca musi skierować do realizacji zamówienia dedykowany zespół składający się z minimum 2 osób, które wspólnie posiadają kwalifikacje niezbędne do rzetelnego wykonania całości przedmiotu zamówienia, realizujący następujące role:

Rola nr 1: Audyt wstępny/końcowy

Osoba ta musi: Posiadać udokumentowane uprawnienia do przeprowadzania audytów bezpieczeństwa informacji zgodnie z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, tj. legitymować się aktualnym, co najmniej jednym z certyfikatów: CISA, CISM, CISSP, CRISC lub certyfikatem Audytora Wiodącego ISO/IEC 27001 wydanym przez akredytowaną jednostkę certyfikującą.

Posiadać doświadczenie w przeprowadzeniu minimum 3 audytów bezpieczeństwa informacji lub wdrożeń SZBI w jednostkach sektora finansów publicznych w ciągu ostatnich 3 lat.

Rola nr 2: Opracowanie/wdrożenie SZBI, warsztaty/szkolenie przedwdrożeniowe dla kierownictwa, szkolenie powdrożeniowe dla pracowników

Osoba ta musi: Posiadać aktualny certyfikat kompetencji personalnych w zakresie systemów zarządzania bezpieczeństwem informacji, tj. legitymować się aktualnym certyfikatem Wdrożeniowca lub Audytora Wiodącego ISO/IEC 27001 wydanym przez akredytowaną jednostkę certyfikującą lub równoważnym aktualnym certyfikatem międzynarodowym potwierdzającym kompetencje w projektowaniu systemów bezpieczeństwa (np. CISM, CISSP, CRISC, CISA).

Posiadać doświadczenie w opracowaniu i wdrożeniu minimum 3 systemów SZBI w jednostkach sektora finansów publicznych w ciągu ostatnich 3 lat, w tym doświadczenie w tworzeniu planów ciągłości działania (BCP) i planów odtwarzania awaryjnego (DRP).

Rola nr 3: Osoba przeprowadzająca szkolenie z cyberbezpieczeństwa dla pracowników.

Osoba ta musi: Posiadać aktualny międzynarodowy lub krajowy certyfikat potwierdzający specjalistyczną wiedzę z zakresu cyberbezpieczeństwa (np. CompTIA Security+, CEH, CISM, CISSP, CRISC, Wdrożeniowiec lub Audytor Wiodący ISO/IEC 27001 lub równoważny) oraz wykazać się osobistym przeprowadzeniem w ciągu ostatnich 3 lat minimum 3 szkoleń/prelekcji z zakresu cyberbezpieczeństwa, bezpieczeństwa informacji lub systemów teleinformatycznych dla grup liczących minimum 20 osób każda.

Zamawiający dopuszcza łączenie powyższych ról przez poszczególnych członków zespołu pod warunkiem bezwzględnego zapewnienia minimum dwuosobowego składu osobowego całego zespołu realizującego zamówienie.

Wykonawca zobowiązany jest dołączyć do oferty wypełniony Wykaz osób, stanowiący załącznik nr 5 do zapytania ofertowego, w którym wskaże imienny skład zespołu wraz z wykazem posiadanych certyfikatów/uprawnień/doświadczenia.

Działając w oparciu o art. 44 ust. 3 ustawy o finansach publicznych oraz mając na względzie szczególny charakter zamówienia związany z bezpieczeństwem teleinformatycznym Urzędu, Zamawiający zastrzega, że kluczowe części zamówienia, tj. przeprowadzenie audytów, opracowanie SZBI, prace wdrożeniowe SZBI, muszą zostać wykonane bezpośrednio przez Wykonawcę. Zamawiający wyłącza w tym zakresie możliwość powierzenia prac podwykonawcom (podmiotom trzecim). Osoby wyznaczone do realizacji zamówienia, składające się na dedykowany zespół ekspercki wskazany w załączniku nr 5 do zapytania ofertowego (z wyjątkiem osoby przeprowadzającej szkolenie z cyberbezpieczeństwa) muszą być na czas trwania umowy związane bezpośrednio z Wykonawcą stosunkiem prawnym umożliwiającym realizację zadań (np. umowa o pracę, umowa cywilnoprawna lub stały kontrakt B2B).