Fundusze Europejskie na Rozwój Cyfrowy

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Nazwa zamówienia:

opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji wraz audytami dokumentacji, audytami sieci oraz szkoleniami w ramach projektu pn. „Cyberbezpieczny samorząd”.

Adres: Miasto i Gmina Pleszew, ul. Rynek 1, 63-300 Pleszew.

Wspólny Słownik Zamówień Publicznych CPV:

72222000-7 Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej oraz usługi w zakresie planowania

79417000-0 Usługi doradcze w zakresie bezpieczeństwa

80000000-4 Usługi edukacyjne i szkoleniowe

Zamawiający: Miasto i Gmina Pleszew, ul. Rynek 1, 63-300 Pleszew.

Opis przedmiotu zamówienia:

Przedmiot zamówienia obejmuje wykonanie następujących usług:

Zadanie 1 – Audyt bezpieczeństwa sieci Urzędu Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew.

Zadaniem jest przeprowadzenie audytu polegającego na badaniu podatności sieci komputerowej na próby ataków pod kątem luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych oraz konfiguracji. Celem audytu jest określenie faktycznego stanu bezpieczeństwa struktur sieci LAN/ WAN, oraz wykrycia naruszeń bezpieczeństwa sieci.

Zakres audytu bezpieczeństwa powinien obejmować co najmniej:

- analizę topologii sieci ,
- weryfikację podziału LAN na strefy,
- określenie usług działających w sieci LAN,
- poszukiwanie podatności (luki poziomu krytycznego, wysokiego, średniego, rekomendacje),
- szczegółową analizą wybranej komunikacji sieciowej,
- weryfikację dostępnych mechanizmów uwierzytelniania dostępnych w sieci,
- weryfikację dostępu do Internetu z LAN,
- wskazanie potencjalnych, dodatkowych metod ochrony sieci,
- wykrywanie udostępnionych w sieci dokumentów pakietu Microsoft Office,
- udostępnione zasoby,
- politykę haseł – GPO, kont użytkowników,
- hasła domyślne urządzeń - analizę urządzeń w Organizacji pod kątem domyślnych ustawień/ poświadczeń,
- analizę bezpieczeństwa sieci zewnętrznej - analizowanie Organizacji z zewnątrz,
- pobranie adresu zewnętrznego IP Organizacji,
- poszukiwanie podatności zewnętrznego adresu IP.

Audyt musi być zakończony przedstawieniem opracowanego raportu zawierającego wykryte podatności podzielone i przypisane, według wielkości zagrożenia oraz zawierać opis rekomendowanych działań zapobiegawczych zmierzających do wyeliminowania i/ lub ograniczenia podatności oraz wszelkich rozwiązań podnoszących poziom ochrony sieci.

Raport zostanie opracowany odrębnie dla każdej jednostki organizacyjnej (UMIG, CUS, CUW).

Do badań podatności wykonawca musi używać oprogramowania komercyjnego, na które przedstawi dowód licencyjny/zakupu oprogramowania.

Zadanie 2 – opracowanie Systemu Zarządzania Bezpieczeństwem Informacji wraz z Analizą Ryzyka i Planem Ciągłości Działania systemów IT dla Urzędu Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew.

Etap I

Wykonanie analizy wstępnej posiadanego Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew.

Wykonawca przeprowadzi analizę, której celem jest identyfikacja kontekstu SZBI u Zamawiającego, obejmującą w szczególności:

a) obszary działalności Zamawiającego i realizowanych zadań,
b) strukturę organizacyjną Zamawiającego,
c) specyfikę pracy poszczególnych komórek organizacyjnych Zamawiającego,
d) systemy informatyczne użytkowane przez Zamawiającego,
e) rejestry publiczne pozostające we właściwości Zamawiającego,
f) SZBI aktualnie funkcjonujący u Zamawiającego,
g) wstępną identyfikację informacji przetwarzanych u Zamawiającego,

h) wstępną identyfikację ryzyk związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego

Analiza musi być zakończona przedstawieniem raportu pozwalającego stwierdzić Zamawiającemu, na jakim poziomie jest zarządzanie bezpieczeństwem informacji oraz jakie obszary powinien jeszcze doskonalić, aby osiągnąć gotowość do wdrożenia dobrych praktyk w oparciu o normę ISO 27001, rozporządzenie KRI oraz ustawie o Krajowym Systemie Cyberbezpieczeństwa. Analiza umożliwi określenie struktury dokumentacji nowego SZBI, która powinna mieć układ hierarchiczny, tj. opisywać nowy SZBI na różnych poziomach szczegółowości oraz określać zagadnienia, które muszą zostać obligatoryjnie uregulowane.

Raport zostanie opracowany odrębnie dla każdej jednostki organizacyjnej (UMIG, CUS, CUW).

Etap II

Opracowanie Systemu Zarządzania Bezpieczeństwem Informacji wraz z Analizą Ryzyka i Planem Ciągłości Działania systemów IT dla Urzędu Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew.

1. Stworzony SZBI powinien być zgodny z rozporządzeniem KRI i spełniać wymagania normy PN-ISO/IEC 27001, w tym obejmować czternaście następujących obszarów mających wpływ na bezpieczeństwo w organizacji Zamawiającego:
    1) Polityka Bezpieczeństwa,
    2) Organizacja bezpieczeństwa informacji,
    3) Bezpieczeństwo zasobów ludzkich,
    4) Zarządzanie aktywami,
    5) Kontrola dostępu,
    6) Kryptografia,
    7) Bezpieczeństwo fizyczne i środowiskowe,
    8) Bezpieczna eksploatacja,

9) Bezpieczna komunikacja,
10) Pozyskiwanie, rozwój i utrzymanie systemów,
11) Relacje z dostawcami,
12) Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
13) Aspekty bezpieczeństwa w zarządzaniu ciągłością działania,
14) Zgodność z wymaganiami prawnymi i własnymi standardami.

2. Stworzony SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:
   - rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773);
   - 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) (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 (t.j. Dz.U. z 2024 r. poz. 307);
   - ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r. poz. 902);
   - ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2024 r. poz. 632);
   - ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r. poz. 1077);

- dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.
- oraz uwzględniać wewnętrzne akty prawne obowiązujące u Zamawiającego.

3. W ramach opracowania nowego SZBI Wykonawca między innymi:
   1) zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią raportu z etapu I zaakceptowanego przez Zamawiającego;
   2) uwzględni w szczególności następujące zagadnienia:
      - określenie organizacji bezpieczeństwa informacji,
      - identyfikacja aktywów informacyjnych i klasyfikacja informacji przetwarzanych u Zamawiającego,
      - szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
      - bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
      - kontrola dostępu,
      - bezpieczeństwo fizyczne i środowiskowe,
      - klasyfikacja informacji,
      - odpowiedzialność za zasoby,
      - postępowanie z nośnikami informacji,
      - użytkowanie urządzeń mobilnych i praca zdalna,
      - zarządzanie sprzętem informatycznym,
      - instalacja oprogramowania,
      - ochrona przed złośliwym oprogramowaniem,
      - kopie zapasowe,
      - zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
      - zarządzanie dokumentacją infrastruktury informatycznej,
      - monitorowanie systemów informatycznych,

- zarządzanie pojemnością,
- serwis i konserwacja infrastruktury informatycznej,
- zarządzanie podatnościami technicznymi,
- zarządzanie incydentami bezpieczeństwa,
- zabezpieczenia kryptograficzne,
- bezpieczeństwo sieci i transmisji danych,
- ochrona własności intelektualnej,
- bezpieczeństwo informacji w relacjach z dostawcami,
- ciągłość działania,
- zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
- weryfikacja zgodności z wymaganiami prawnymi,
- korzystanie z poczty elektronicznej i Internetu,
- zarządzanie usługami informatycznymi,
- utrzymanie i doskonalenie SZBI,
- przeprowadzanie audytów SZBI.

W/w zagadnienia zostaną dopasowane do potrzeb danej jednostki oraz wewnętrznych regulacji i rozwiązań.

Po przeprowadzonej analizie ryzyka, zostanie udostępnione narzędzie oraz metodyka do samodzielnej analizy.

Wymagania dotyczące spotkań projektowych: Liczba spotkań projektowych w każdej jednostce wynosi minimum 2-3 udokumentowane spotkania z kadrą kierowniczą. Spotkania te mają na celu zebranie informacji niezbędnych do opracowania indywidualnych procedur oraz omówienie specyficznych potrzeb i wymagań każdej jednostki.

Dokumentacja SZBI zostanie opracowana odrębnie dla każdej jednostki organizacyjnej (UMIG, CUS, CUW).

Zadanie 3 – Audyt wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew.

Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji, zgodnie z poniższymi warunkami:

1) zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, ustawy o krajowym systemie cyberbezpieczeństwa oraz zgodność z wymaganiami normy PN-ISO/IEC 27001;
2) raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST i dostarczony do Zleceniodawcy. Raport zostanie opracowany odrębnie dla każdej jednostki organizacyjnej (UMIG, CUS, CUW).
3) audyt systemu bezpieczeństwa informacji wdrożonego u Zamawiającego musi zostać przeprowadzony przez:
   a) audytora zewnętrznego posiadającego 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) lub;
   b) audytora wewnętrznego posiadającego 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) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;

Zadanie 4 – szkolenia dla kadry kierowniczej Urzędu Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew z opracowanego Systemu Zarządzania Bezpieczeństwem Informacji wraz z Analizą Ryzyka oraz procedur bezpieczeństwa systemów IT.

Ilość osób do przeszkolenia: UMiG 22, CUS 6, CUW 2

Zamawiający zastrzega, że liczba ta może się zmienić o +/- 10%, w związku z rotacją pracowników.

Wykonawca musi przeprowadzić 2 szkolenia dla kadry kierowniczej w/w jednostek. Szkolenie musi obejmować m.in.:

1. wymogi wynikające z KRI, UoKSC i RODO
2. zarządzanie ryzykiem w bezpieczeństwie informacji
3. System Zarzadzania Bezpieczeństwem informacji – jak skutecznie przestrzegać procedur wdrożonej Polityki Bezpieczeństwa Informacji.
4. Ciągłość działania – dlaczego jest istotna i jak ją wdrożyć
5. Identyfikowanie zagrożeń – jak wdrożyć odpowiednie rozwiązania na przestrzeganie zasad bezpieczeństwa
6. Przegląd znanych typów ataków na JST - najnowsze zagrożenia.

Zadanie 5 - Szkolenia z cyberbezpieczeństwa dla pracowników Urzędu Miasta i Gminy w Pleszewie oraz dla jednostek organizacyjnych – tj. Centrum Usług Społecznych w Pleszewie oraz Centrum Usług Wspólnych Miasta i Gminy Pleszew.

Ilość osób do przeszkolenia: UMiG 115, CUS 35, CUW 14

Zamawiający zastrzega, że liczba ta może się zmienić o +/- 10%, w związku z rotacją pracowników.

Szkolenie musi być przeprowadzone w grupach maksymalnie 45 osobowych.

Wykonawca musi przeprowadzić 2 szkolenia dla pracowników w/w jednostek. Szkolenie musi obejmować m.in.:

1. Podstawy prawne i główne zasady cyberbezpieczeństwa
2. Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
    a. Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa
    b. Wymagania dla pracowników wynikające z KRI, UoKSC oraz RODO
    c. System Zarządzania Bezpieczeństwem Informacji w praktyce
3. Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
    a. Ochrona informacji i prywatność w internecie
    b. Ransomware jako poważne zagrożenie dla JST
    c. Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise)
    d. Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne
    e. Bezpieczne hasła i uwierzytelnienie dwuskładnikowe
    f. Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa

Wymagania dotyczące doświadczenia oraz kompetencji wykonawców usług

Wykonawca musi posiadać przynajmniej dwuletnie doświadczenie w przeprowadzaniu projektów w obszarze cyberbezpieczeństwa, audytów KRI oraz przedstawić stosowne referencje od podmiotów publicznych.

1. Osoba przeprowadzająca Audyt bezpieczeństwa sieci musi posiadać 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).

Kopię certyfikatu należy dołączyć do oferty.

2. Aby zapewnić zastępowalność audytorów oraz gwarancję wykonania usług, Wykonawca powinien posiadać w zespole projektowym wyznaczonym do wykonania zamówienia co najmniej trzy osoby legitymujące się certyfikatami Audytora Wiodącego nomy ISO 27001 zgodnego z akredytacją PCA (Polskie Centrum Akredytacji).

3. Wykonawca powinien wykazać się osobami w zespole projektowym posiadającymi dyplomy/certyfikaty:

- Dyplom ukończenia studiów podyplomowych z zarządzania cyberbezpieczeństwem.
- Certyfikat Auditora wewnętrzny systemu zarządzania ciągłością działania wg ISO 22301:2019
- Zarządzania Ryzykiem w Systemie Zarządzania Bezpieczeństwem Informacji wg ISO 27005

4. Wykonawca załączy do oferty pisemne referencje lub inne dowody od podmiotów JST, z których wynika, że przeprowadzono usługi były w okresie ostatnich 3 lat realizowane należycie z zakresu:

- audytów bezpieczeństwa sieci – minimum 5
- opracowania polityki bezpieczeństwa Informacji - minimum 5
- szkoleń z cyberbezpieczeństwa– minimum 5

5. Wykonawca powinien posiadać kopię polisy odpowiedzialności cywilnej na świadczone obowiązki na kwotę co najmniej 1 000 000 zł.

Kopię polisy Wykonawca załącza do oferty

6. Wykonawca powinien posiadać w zakresie wykonywania szkoleń certyfikat SUS 2.0. lub równoważny, który określa wymagania wobec firm szkoleniowych w zakresie przygotowania, realizacji i ewaluacji oferowanych usług.

Kopię certyfikatu wykonawca załącza do oferty. Dodatkowo powinien wykazać wpis do Rejestru Instytucji Szkoleniowych.

7. Wykonawca zobowiązuje się do wykonania niniejszej usługi za pomocą własnych zasobów.
8. Wykonawca zapewni konsultacje w zakresie przeprowadzonych usług do 12 m-cy po przeprowadzonych usługach.