Załącznik nr 1 zapytania ofertowego

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest opracowanie i wdrożenie wspólnej dokumentacji Systemu zarządzania Bezpieczeństwa Informacji (SZBI), wykonanie audytu przedwdrożeniowego i audytu powdrożeniowego w Urzędzie Gminy Stara Kornica, GOPS Stara Kornica i trzech jednostek oświatowych, utrzymanie SZBI oraz świadczenie usługi Pełnomocnika i Audytora SZBI"

1. Przedmiotem zamówienia objęte są jednostki:
2. **Urząd Gminy Stara Kornica,** Stara Kornica 191, 08-205 Kornica (zatrudnionych 37 pracowników)
3. **Gminny Ośrodek Pomocy Społecznej w Starej Kornicy,** Stara Kornica 191, 08-205 Kornica (zatrudnionych 6 pracowników)
4. **Zespół Publicznych Placówek Oświatowych im. Odzyskania Niepodległości w Starej Kornicy,** Stara Kornica 172, 08-205 Kornica (zatrudnionych 53 pracowników)
5. **Szkoła Podstawowa im. Marii Konopnickiej w Kobylanach,** Kobylany 114, 08-205 Kornica (zatrudnionych 18 pracowników)
6. **Szkoła Podstawowa w Starych Szpakach,** Stare Szpaki 36, 08-205 Kornica (zatrudnionych 17 pracowników)
7. Środowisko teleinformatyczne zawiera obecnie około 4 elementów aktywnych sieci, 2 serwery fizyczne, 4 serwery wirtualnych, zlokalizowanych w jednostkach wskazanych powyżej.
8. **Kontekst, założenia dotyczące zamówienia**

Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Zamawiającego poprzez określenie do wdrożenia niezbędnych elementów Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami ujętymi w: ISO/IEC 27001:2022 (PN-ISO/IEC 27001:2023), PN- ISO/IEC 27005:2022, PN-ISO/IEC 22301:2020 wynikających z przepisów prawa dla jednostek wskazanych powyżej.

**Zamawiający przewiduje w ramach przedmiotu zamówienia 3 części realizacji:**

**Część 1: opracowanie i wdrożenie wspólnej dokumentacji Systemu zarządzania Bezpieczeństwa Informacji (SZBI) dla Urzędu Gminy i GOPS oraz jednostek oświatowych według najnowszej obowiązującej polskiej normy PN EN ISO/IEC 27001:2023**

Poprzez opracowanie dokumentacji SZBI należy rozumieć: przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej spełniającej wymagania normy ISO/IEC 27001, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego. Opracowana dokumentacja musi być zgodna 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,
* ustawą z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. z 2024 r. poz. 1077 z późn. zm.),
* rozporządzeniem 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),
* dyrektywą 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) oraz akty wykonawcze wydane do niej

W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta nowelizacja wyżej wymienionych przepisów prawa lub zostaną opublikowane akty wykonawcze do dyrektywy NIS2. Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy opracowaniu i wdrażaniu dokumentacji SZBI.

Opracowanie przez Wykonawcę niżej wymienionych dokumentów, przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej do stanu, który pozwala przekazać dokumenty jednostce certyfikującej, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego. Po stronie Zamawiającego leży jedynie uzgodnienie treści dokumentów z Wykonawcą.

* 1. **Klasyfikacja informacji przetwarzanych u Zamawiającego**

W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:

* opracowanie metodyki klasyfikowania informacji przetwarzanych u Zamawiającego;
* opracowanie modelu podziału informacji przetwarzanych u Zamawiającego w zależności od poziomu ich wrażliwości i przeznaczenia;
* sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych u Zamawiającego;
* opracowanie raportu z procesu klasyfikacji informacji.
  1. **Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego zgodnie z wytycznymi normy PN-ISO/IEC 27005:2022**

W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego, a w szczególności:

* opracować metodykę szacowania ryzyka spełniającą wymagania PN-ISO/IEC 27005:2022,

optymalną ze względu na charakter działalności Zamawiającego;

* opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
* przeprowadzić wspólnie z wyznaczonymi pracownikami Zamawiającego proces szacowania ryzyka, w tym:
  + zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
  + opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Zamawiającego;
  + opracować przy współudziale wyznaczonych pracowników Zamawiającego plan postępowania z ryzykiem.
  1. **Opracowanie dokumentów niezbędnych do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji**

Opracowanie dokumentów niezbędnych do wdrożenia systemu zarządzania bezpieczeństwem informacji wraz z przekazaniem praw autorskich do ww. dokumentów, zgodnie z wymaganiami:

* + 1. ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
    2. 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,
    3. ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa,
    4. normy PN-ISO/IEC 27001:2023.

Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest przedstawić elementy niezbędne do opracowania dokumentacji SZBI przez Zamawiającego a także wytypować procesy niezbędne do poprawnego funkcjonowania organizacji.

Wykonawca gwarantuje, że opracowana przez niego dokumentacja systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy ISO/IEC 27001 oraz wymaganiami certyfikacyjnymi jednostki certyfikującej systemy zarządzania na zgodność z normą ISO/IEC 27001, akredytowanej przez Polską jednostkę akredytującą wymienioną na stronie [http://www.iaf.nu//articles/IAF\_MEMBERS\_SIGNATORIES/4](http://www.iaf.nu/articles/IAF_MEMBERS_SIGNATORIES/4).

W skład dokumentacji SZBI w szczególności wchodzą następujące polityki i procedury:

1. Polityka bezpieczeństwa informacji - definiująca jej cele strategiczne, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa.
2. Księga systemu zarządzania bezpieczeństwem informacji, zawierająca ogólny opis elementów SZBI, zasady: wdrożenia, stosowania, monitorowania, przeglądu, utrzymania i doskonalenia SZBI klasyfikację informacji, schemat organizacyjny kierowania sprawami bezpieczeństwa informacji.
3. Mapa procesów objętych SZBI minimum 6 procesów (min. proces zarządzania i utrzymania SZBI, proces zarządzania ryzykiem, proces zarządzania incydentami (RODO, UoKSC), proces zarządzania dostawami (wybór-realizacja-zakończenie współpracy), proces zarządzania pracownikami (rekrutacja-zatrudnienie-zwolnienie), proces obsługi interesanta (obsługa wniosków). Schemat procesów należy przygotować w notacji BPMN (forma edytowalna).
4. Deklaracja stosowania zabezpieczeń dla systemu bezpieczeństwa informacji wraz z przyporządkowanie aktualnie używanych w organizacji rozwiązań do wymagań normy.
5. Metodyka szacowania ryzyka zgodnie z wymaganiami normy ISO27005:2022.
6. Polityka ochrony danych osobowych (lub jej dostosowanie).
7. Polityka i plany ciągłości działania (BCP) zgodny z wymaganiami określonymi w normie ISO 22301:2019.
8. Wszystkie procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, niezbędne do prawidłowego funkcjonowania SZBI:
   * Procedura nadzoru nad dokumentami
   * Procedura działań doskonalących, korygujących i zapobiegawczych
   * Procedura audytu wewnętrznego
   * Procedura nadzoru nad zapisami
   * Procedura przeglądu zarządzania
   * Procedura zarządzania incydentami
   * Procedura bezpieczeństwa wewnętrznego organizacji
   * Procedura ewakuacji personelu i sprzętu z obiektów
   * Procedura klasyfikacji informacji wewnętrznych i zewnętrznych
   * Procedura oceny ryzyk generowanych przez strony zewnętrzne (klientów, dostawców, kooperantów, innych)
   * Procedura postępowania w przypadku odejścia pracownika z firmy
   * Procedura bezpieczeństwa infrastruktury teleinformatycznej (sieć, serwerownie, urządzenia łączności, inne elementy)
   * Procedura bezpieczeństwa fizycznego
   * Procedura pomiaru skuteczności SZBI
   * Dokumenty ustalające status systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy
   * Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji
   * Opracowanie formularzy i rejestrów będących integralną częścią w/w dokumentów w formie i treści odpowiedniej do potrzeb i woli Zamawiającego (zawartość merytoryczna oraz forma)
   * Inne niezbędne u Zamawiającego z punktu widzenia systemu bezpieczeństwa informacji (po ocenie potrzeb)
   1. **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji**
9. Analiza ryzyka u Zamawiającego zgodnie z wymaganiami normy ISO27005:2022:
   * Identyfikacja aktywów informacyjnych
   * Identyfikacja zagrożeń
   * Identyfikacja i ocena podatności, które mogą być wykorzystane przez zagrożenia dla aktywów
   * Identyfikacja i ocena skutków utraty poufności, integralności i dostępności w odniesieniu do aktywów
   * Ocena ryzyka
10. Analiza ryzyka u Zamawiającego zgodnie z wymaganiami normy ISO222301(BIA)
11. Wdrożenie dokumentów do stosowania, a w szczególności:
    * + przygotowanie i przekazanie wytycznych odnośnie do elektronicznego nadzorowania dokumentów i zapisów, jeżeli potrzebne, konfiguracja ustawień
      + uzupełnienia zapisów wymaganych normą razem z Zamawiającym
      + konsultacje indywidualne z zakresu stosowania opracowanej dokumentacji
      + udzielenie wszelkiego wsparcia w celu uzyskania biegłego posługiwania się przez Zamawiającego systemem (nie mniej niż 20 godzin zegarowych)

Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.

Wykonawca zobowiązany jest do zachowania w poufności informacji uzyskanych na etapie opracowania i wdrożenia SZBI w jednostkach na podstawie odrębnej umowy o powierzenie przetwarzania danych osobowych.

Opracowana dokumentacja zostanie przekazana Zamawiającemu w formie edytowalnych plików w formacie Word/Excel.

Dokumentacja musi zawierać wszystkie niezbędne polityki i procedury, dokumenty niezbędne do zarządzania bezpieczeństwem informacji, instrukcje, metodologie zarządzania ryzykiem, wzory wniosków, matryce itd.

Po opracowaniu i zaakceptowaniu przez Zamawiającego dokumentacji wewnętrznej SZBI Wykonawca przeprowadzi w formie zdalnej instruktaż dla pracowników jednostek w celu zaznajomienia ich z zapisami SZBI. Wykonawca przekaże Zamawiającemu nagranie z przeprowadzonego instruktażu.

Pracownicy powinni zdobyć wiedzę na temat zasad ochrony informacji w organizacji oraz roli, jaką pełnią w utrzymaniu i przestrzeganiu SZBI. Celem jest podniesienie świadomości dotyczącej bezpieczeństwa informacji, ryzyka związanych z ich przetwarzaniem oraz zagrożeń cybernetycznych.

1. **Zakres tematyczny**:
   * **Podstawy SZBI**: Wprowadzenie do norm i standardów związanych z bezpieczeństwem informacji (np. ISO/IEC 27001, RODO, itp.).
   * **Polityki bezpieczeństwa informacji**: Omówienie głównych polityk organizacji w zakresie ochrony danych i informacji.
   * **Ryzyka i zagrożenia**: Analiza typowych zagrożeń związanych z bezpieczeństwem informacji oraz technik wykorzystywanych przez cyberprzestępców.
   * **Procedury ochrony informacji**: Przedstawienie procedur dotyczących klasyfikacji, przetwarzania i przechowywania informacji w sposób bezpieczny.
   * **Rola pracownika w SZBI**: Zrozumienie odpowiedzialności pracowników za przestrzeganie zasad SZBI, w tym odpowiednie zarządzanie hasłami, szyfrowanie danych oraz zgłaszanie nieprawidłowości.
   * **Zarządzanie incydentami bezpieczeństwa**: Procedury postępowania w przypadku wykrycia incydentu związane z bezpieczeństwem informacji (np. ataków cybernetycznych, wycieków danych).
   * **Prawo i regulacje dotyczące ochrony danych i informacji**: Omówienie przepisów prawnych i regulacyjnych, które wpływają na zarządzanie danymi i informacjami w organizacji
   1. **Zapoznanie osób zarządzających z Systemem Zarządzania Bezpieczeństwem Informacji:**

Celem jest przekazanie uczestnikom wiedzy o roli kierownictwa w zapewnieniu skutecznego zarządzania bezpieczeństwem informacji, umożliwiającego pełne wdrożenie i ciągłe doskonalenie SZBI w organizacji. Uczestnicy powinni zrozumieć swoje obowiązki związane z nadzorowaniem polityki bezpieczeństwa oraz wprowadzać działania zapewniające zgodność z normami i regulacjami.

1. **Zakres tematyczny**

* **Wprowadzenie do SZBI**: Przegląd podstawowych pojęć związanych z bezpieczeństwem informacji, normy ISO/IEC 27001, wymagania RODO, oraz znaczenie SZBI w kontekście organizacyjnym.
* **Rola kierownictwa w SZBI**: Omówienie odpowiedzialności osób zarządzających jednostką w zakresie wdrożenia, monitorowania i oceny skuteczności SZBI. Zrozumienie roli liderów w tworzeniu kultury bezpieczeństwa w organizacji.
* **Planowanie i strategia SZBI**: Jak stworzyć i wdrożyć długoterminową strategię bezpieczeństwa informacji, uwzględniając cele biznesowe i ryzyka związane z bezpieczeństwem informacji.
* **Zarządzanie ryzykiem w SZBI**: Zrozumienie procesów oceny, analizy i zarządzania ryzykiem bezpieczeństwa informacji. Omówienie narzędzi i metod służących identyfikowaniu zagrożeń oraz wdrażania działań zaradczych.
* **Polityki i procedury**: Jak opracować i wdrożyć polityki bezpieczeństwa informacji oraz procedury operacyjne w zakresie ochrony danych i informacji. Przykłady polityk bezpieczeństwa, zarządzanie dostępem, zasady ochrony danych osobowych, zarządzanie incydentami.
* **Zgodność z regulacjami**: Zrozumienie przepisów prawnych i regulacji, takich jak RODO, które mają wpływ na politykę bezpieczeństwa informacji w organizacji. Jak zapewnić zgodność z wymogami prawnymi oraz audyty wewnętrzne.
* **Monitorowanie i audyt SZBI**: Nadzór nad monitorowaniem efektywności SZBI, w tym rola audytów wewnętrznych i zewnętrznych w utrzymaniu zgodności z wymaganiami. Jak przeprowadzać ocenę ryzyka i analizę bezpieczeństwa.
* **Reagowanie na incydenty i ciągłość działalności**: Opracowanie planów reagowania na incydenty związane z bezpieczeństwem informacji. Jak stworzyć i wdrożyć plan ciągłości działania oraz plan odzyskiwania po awarii (disaster recovery).

1. **Doskonalenie SZBI**: Strategie wprowadzania ciągłych usprawnień w systemie zarządzania bezpieczeństwem informacji. Jak śledzić zmiany w technologii, przepisach prawnych i zagrożeniach, oraz dostosować SZBI do nowych wyzwań.

**Część 2: wykonanie audytu przedwdrożeniowego i audytu powdrożeniowego w Urzędzie Gminy Stara Kornica, GOPS Stara Kornica i trzech jednostek oświatowych**

Przeprowadzone audyty pozwolą na weryfikacje bezpieczeństwa danych, audyt ponadto pozwoli na sprawdzenie aktualności oprogramowania i sprzętu, które wykorzystywane są do przetwarzania informacji. Audyt koncentruje się także na przeprowadzeniu analizy ryzyka utraty integralności, dostępności czy poufności informacji oraz ma za zadanie wskazać działania, które zminimalizują ryzyko.

**Ogólne wymagania odnośnie do audytów**

Audyty zostaną przeprowadzone w lokalizacjach jednostek Zamawiającego. Za zgodą Zamawiającego zdalnie można wykonywać czynności uzupełniające – np. przesyłanie materiałów lub wyjaśnień. Łączny czas trwania audytów nie może być krótszy niż 20 godzin.

* + Audyt Techniczny – wymagań zawartych w załączniku A normy ISO/IEC 27001
  + Audyt Systemowy – wymagań normy zawartych normie ISO/IEC 27001
  + Sporządzenie raportów w formie pisemnej (edytowalnej i nieedytowalnej
  + Przekazanie raportów do Zamawiającego
  + Wykonanie razem z Zamawiającym działań poaudytowych, w formie uzgodnionej   
    z Zamawiającym. Jeżeli występuje konieczność korekty dokumentacji, wykonuje ją Wykonawca.
  1. **Audyt przedwdrożeniowy – ma na celu wykrycie ewentualnych podatności i luk w posiadanych systemach i oprogramowaniu, wykonanie analizy ryzyka.**

**Audyt bezpieczeństwa systemów informacyjnych**

Przeprowadzenie audytu bezpieczeństwa w oparciu o wymagania załącznika A do normy ISO 27001 oraz wytycznych normy ISO 27002 w zakresie bezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usług dla klientów jednostek.

Audyt powinien zawierać także wskazania podatności systemów informatycznych: wskazanie podatności, wagi podatności, opis podatności, informacje dotyczące podatności w tym źródła zewnętrzne, rekomendacje co do sposobu postępowania

Wykonawca przy wykonywaniu umowy może oprócz audytorów wskazanych w formularzu ofertowym dodatkowo posiłkować się innymi pracownikami i współpracownikami Wykonawcy. Powierzenie wykonania części przedmiotu Umowy innym pracownikom i współpracownikom nie wymaga uprzedniej zgody Zamawiającego, przy czym Wykonawca odpowiada za działania osób trzecich jak za działania własne.

Wykonawca dostarczy Zamawiającemu raport z audytu. Powyższe dokumenty należy przygotować oddzielnie dla każdej jednostki.

**2) Wykonanie audytu powdrożeniowego**

Usługa będzie obejmować swoim zakresem:

- audyt powdrożeniowy SZBI Zamawiającego,

- audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług przez listę jednostek wymienionych powyżej,

- audyt systemów informacyjnych wykorzystywanych przez Zamawiającego we wskazanych w liście powyżej lokalizacjach,

- Audyt Ciągłości Działania – wymagań normy zawartych normie ISO/IEC 22301.

**Część 3: utrzymanie SZBI oraz usługi Pełnomocnika i Audytora SZBI**

**Usługa pełnomocnika (1 osoba):**

- Koordynowanie systemu bezpieczeństwa: pełnomocnik odpowiada za wdrażanie, utrzymanie i doskonalenie SZBI. Realizacje zadania związane z zapewnieniem zgodności z ustawą o krajowym systemie cyberbezpieczeństwa Krajowymi Ramami Interoperacyjności oraz innymi przepisami prawa i zgodnie z normą PN EN ISO/IEC 27001:2023

- analiza ryzyka i planowanie działań

- współpraca z kadrą zarządzającą i pracownikami: koordynuje wdrażanie wewnętrznych polityk i procedur bezpieczeństwa, a także monitoruje poziom ich przestrzegania.

- komunikacja i raportowanie: pełnomocnik prowadzi kontakty w obszarze bezpieczeństwa informacji, współdziała z audytorem oraz właściwymi organami. Raportuje do kierownictwa o zagrożeniach i postępach w zakresie wdrażania SZBI.

**Usługa Audytora SZBI (1 osoba):**

- wykonanie audytu przedwdrożeniowego i audytu powdrożeniowego w Urzędzie Gminy Stara Kornica, GOPS Stara Kornica i trzech jednostek oświatowych