



Opis Przedmiotu Zamówienia (zwany „OPZ”)

I. Ogólne warunki realizacji zamówienia

1. Przedmiotem zamówienia jest opracowanie przez Wykonawcę dla Zamawiającego nowego systemu zarządzania bezpieczeństwem informacji, zwanego „nowym SZBI”, i przeprowadzenie szkoleń, zwanych „Szkoleniami”, oraz przekazanie materiałów szkoleniowych m.in. w zakresie jego funkcjonowania, a także świadczenie usług asysty wdrożeniowej, zwanych „Usługami asysty”, zgodnie z Umową, zwane „Przedmiotem Umowy”.
2. Przedmiot Umowy będzie realizowany w trzech etapach:
 - 1) **Etap I** – analiza działalności Zamawiającego i sporządzenie Sprawozdania, o którym mowa w tyt. II ust. 1 pkt 2;
 - 2) **Etap II** – opracowanie nowego SZBI;
 - 3) **Etap III** – świadczenie Usług asysty wdrożeniowej, zwanych dalej „Etapami”, które szczegółowo określa niniejszy OPZ.
3. Wykonawca zobowiązuje się wykonać Przedmiot Umowy w terminach określonych w Umowie.

II. ETAP I

1. W ramach Etapu I Wykonawca:
 - 1) przeprowadzi analizę, zwaną dalej „Analizą”, 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
– w ramach której Wykonawca dokona oceny ryzyk i szans niezbędnych do zaprojektowania nowego SZBI – również poprzez weryfikację działalności Zamawiającego m.in. w jego siedzibie
 - 2) sporządzi sprawozdanie, zwane dalej „Sprawozdaniem”:
 - a) podsumowujące przeprowadzoną Analizę, w zakresie, o którym mowa w ust. 1 pkt 1,
 - b) obejmujące propozycje rozwiązań i zmian w zakresie bezpiecznego przetwarzania informacji u Zamawiającego i wprowadzenia u niego nowego SZBI,
 - c) obejmujące wstępną koncepcję nowego SZBI, dostosowaną do potrzeb Zamawiającego, w tym do ryzyk właściwych dla Zamawiającego, zidentyfikowanych w wyniku Analizy, w szczególności wskazującą na główne obszary i rodzaje procedur, które powinny zostać uregulowane nowym SZBI.
2. W celu przeprowadzenia Analizy Zamawiający udostępni Wykonawcy niezbędne, posiadane dokumenty, w szczególności dotyczące aktualnie funkcjonującego SZBI.
3. Sprawozdanie zostanie przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.
4. Celem opracowania przez Wykonawcę wstępnej koncepcji nowego SZBI, Zamawiający wskazuje poniżej ogólny ramowy zarys nowego SZBI:
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:
 - 1) poziom jednostki (Zamawiający) – nadrzędny dokument „Polityka Bezpieczeństwa Informacji” Zamawiającego, który określa wymagania i zasady bezpieczeństwa informacji obowiązujące u Zamawiającego oraz sposób organizacji nowego SZBI – z tym dokumentem powinny być spójne pozostałe dokumenty składające się na dokumentację nowego SZBI,
 - 2) poziom systemów teleinformatycznych – polityka bezpieczeństwa systemów teleinformatycznych, na którą składają się:



- ☐ dokument „Polityka Bezpieczeństwa Systemów Teleinformatycznych”, który opisuje wymagania i zasady bezpieczeństwa dla systemów teleinformatycznych,
 - ☐ odniesienia co do wymagań dotyczących zakresu dokumentacji poszczególnych systemów teleinformatycznych – np. dokumenty: polityki bezpieczeństwa poszczególnych systemów teleinformatycznych, które opisują w jaki sposób zasady i wymagania bezpieczeństwa zawarte w „Polityce Bezpieczeństwa Informacji” i „Polityce Bezpieczeństwa Systemów Teleinformatycznych” są realizowane w danym systemie teleinformatycznym,
- 3) poziom procedur, instrukcji i regulaminów – procedury, instrukcje, regulaminy i inne dokumenty SZBI tworzone w celu uszczegółowienia zasad opisanych w ww. politykach, dotyczące w szczególności zagadnień:
- ☐ bezpieczeństwo zasobów ludzkich,
 - ☐ bezpieczeństwo fizyczne,
 - ☐ bezpieczeństwo cyberprzestrzeni,
 - ☐ bezpieczeństwo danych osobowych,
 - ☐ bezpieczeństwo informacji niejawnych,
 - ☐ obsługa incydentów,
 - ☐ zarządzanie ryzykiem,
 - ☐ użytkowanie systemów teleinformatycznych,
 - ☐ użytkowanie urządzeń mobilnych.

Na SZBI będzie się składać dokumentacja zarządzania systemem zarządzania bezpieczeństwem informacji (uwzględniająca poniższe zagadnienia):

- Zasady dotyczące korzystania z systemu zakres, zasoby, ciągłe doskonalenie;
- Procedury przeprowadzania audytów, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.
- Procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania.
- Procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania.
- Procedury przeglądu systemu zarządzania, w szczególności określającej częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków.
- Procedury nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania, zawierające zasady wersjonowania, zatwierdzania, dystrybucji, przechowywania, archiwizowania i niszczenia dokumentów.
- Procedury nadzoru nad udokumentowaną informacją, określającej zasady przechowywania, archiwizowania oraz niszczenia zapisów oraz
- Dokumentacja dotycząca zabezpieczeń systemu zarządzania bezpieczeństwem informacji w obszarach (uwzględniająca poniższe zagadnienia):
 - Zasady bezpiecznego przetwarzania informacji przez pracowników
 - Zabezpieczenie stacji roboczych
 - Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi
 - Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień
 - Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych
 - Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami
 - Zasady publikacji informacji
 - Zasady wymiany danych z podmiotami zewnętrznymi
 - Zasady wewnętrznej wymiany danych
 - Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach
 - Zasady wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych, z uwzględnieniem testowania bezpieczeństwa wprowadzanych rozwiązań



- Wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych
 - Zasady zgłaszania podatności w mechanizmach przetwarzających informacje
 - Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji
 - Zasady kontroli bezpieczeństwa informacji
 - Zasady zarządzania oprogramowaniem
 - Zasady zarządzania kopiami zapasowymi i archiwalnymi
 - Zasady konserwacji i serwisu zabezpieczeń technicznych i systemów informatycznych
 - Zasady monitorowania bezpieczeństwa infrastruktury informatycznej
 - Zasady przygotowania urządzeń IT do ponownego użycia
 - Zasady wycofywania urządzeń IT z użycia
 - Zasady bezpiecznego korzystania z urządzeń mobilnych
 - Zasady bezpiecznej pracy zdalnej
 - Zasady ochrony przed złośliwym oprogramowaniem
 - Zasady zarządzania mechanizmami kryptograficznymi
 - Zasady monitorowania przepisów prawnych związanych z zabezpieczeniem przetwarzanych informacji oraz wprowadzania zmian wynikających z obowiązków prawnych
 - Wytyczne w zakresie ochrony fizycznej i technicznej
 - Wytyczne w zakresie bezpiecznej współpracy z podmiotami zewnętrznymi
 - Wytyczne w zakresie bezpiecznego świadczenia usług związanych z przetwarzaniem informacji
5. Ramowy zarys nowego SZBI, o którym mowa w ust. 4, nie ma charakteru bezwzględnie wiążącego i stanowi jedynie propozycję Zamawiającego. W przypadku nieuwzględnienia przez Wykonawcę we wstępnej koncepcji nowego SZBI ramowego zarysu lub jego poszczególnych elementów, Wykonawca uzasadni powyższe Zamawiającemu.

III. ETAP II

1. W ramach Etapu II Wykonawca, na podstawie wyników Analizy i zaakceptowanego przez Zamawiającego Sprawozdania, opracuje nowy SZBI, dostosowany do potrzeb Zamawiającego.
2. Nowy SZBI, który opracuje Wykonawca, będzie stanowił system zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2021 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. z 2017 r. poz. 2247), bądź w zastępujących go, odpowiednich przepisach wykonawczych do ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2021 r. poz. 2070, z późn. zm.), w przypadku ich nowelizacji, zwany „SZBI”.
Rozporządzenie, o którym mowa w zdaniu poprzedzającym, zwane jest dalej „**rozporządzeniem KRI**”.
3. Nowy 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.

Ponadto, nowy SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762.

4. Nowy SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:
 - 1) rozporządzenia KRI;
 - 2) 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);
 - 3) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
 - 4) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
 - 5) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176, z późn. zm.);
 - 6) ustawy z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowiska (Dz. U. z 2021 r. poz. 2373, z późn. zm.);
 - 7) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742);
 - 8) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z późn. zm.);
 - 9) 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.
5. W ramach opracowania nowego SZBI Wykonawca między innymi:
 - 1) zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;
 - 2) uwzględni w szczególności następujące zagadnienia:
 - a) określenie organizacji bezpieczeństwa informacji,
 - b) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
 - c) szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
 - d) bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
 - e) szkolenia z zakresu bezpieczeństwa informacji,
 - f) kontrola dostępu,
 - g) bezpieczeństwo fizyczne i środowiskowe,
 - h) klasyfikacja informacji,
 - i) odpowiedzialność za zasoby,
 - j) postępowanie z nośnikami informacji,
 - k) użytkowanie urządzeń mobilnych i praca zdalna,
 - l) zarządzanie sprzętem informatycznym,
 - m) instalacja oprogramowania,
 - n) ochrona przed oprogramowaniem złośliwym,
 - o) kopie zapasowe,
 - p) zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
 - q) zarządzanie dokumentacją infrastruktury informatycznej,
 - r) monitorowanie systemów informatycznych,
 - s) zarządzanie pojemnością,
 - t) serwis i konserwacja infrastruktury informatycznej,
 - u) zarządzanie podatnościami technicznymi,
 - v) zarządzanie incydentami bezpieczeństwa,
 - w) zabezpieczenia kryptograficzne,
 - x) bezpieczeństwo sieci i transmisji danych,
 - y) ochrona własności intelektualnej,
 - z) bezpieczeństwo informacji w relacjach z dostawcami,



- aa) ciągłość działania,
 - bb) zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
 - cc) weryfikacja zgodności z wymaganiami prawnymi,
 - dd) korzystanie z poczty elektronicznej i Internetu,
 - ee) zarządzanie usługami informatycznymi,
 - ff) utrzymanie i doskonalenie SZBI,
 - gg) przeprowadzanie audytów SZBI.
6. Wykonawca wraz z nowym SZBI przedstawi zestawienie, zwane „Zestawieniem”, w którym wykaże spełnienie przez nowy SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, w tym rozporządzenia KRI, a także odpowiednich norm.
 7. Nowy SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.
 8. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę nowego SZBI, w tym do rodzaju dokumentów, ich liczby, nazewnictwa, zakresu merytorycznego. Uwagi Zamawiającego powinny być każdorazowo uwzględnione przez Wykonawcę. W przypadku, gdyby proponowane przez Zamawiającego zmiany mogły powodować niezgodność dokumentacji z Umową, Wykonawca poinformuje o tym wcześniej Zamawiającego, uzasadniając swoje stanowisko
– w takim przypadku Zamawiający podejmie ostateczną decyzję w zakresie konieczności uwzględnienia jego uwag przez Wykonawcę.

IV. ETAP III

1. W ramach Etapu III Wykonawca będzie świadczył Usługi wdrożeniowe w następującym zakresie:
 - 1) przeprowadzenie procesów:
 - a) identyfikacji aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
 - b) szacowania ryzyka oraz postępowania z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
– z udziałem wyznaczonych w tym celu pracowników Zamawiającego;
 - 2) wyjaśnianie zagadnień ujętych w nowym SZBI i proponowanie rozwiązań w zakresie jego wdrażania;
 - 3) pomoc w rozwiązywaniu bieżących problemów, które mogą pojawić się w toku funkcjonowania nowego SZBI;
 - 4) pomoc w modyfikacji dokumentacji Zamawiającego związanej z bezpieczeństwem informacji, w szczególności nowego SZBI (np. poprzez zmianę poszczególnych elementów składowych lub opracowanie nowych elementów).
2. Usługi asysty świadczone będą zdalnie (w szczególności za pośrednictwem poczty elektronicznej lub telefonu) lub w siedzibie Zamawiającego. Decyzja o formie świadczenia Usług asysty zależy będzie od ich charakteru i każdorazowo należy do Zamawiającego.
3. Wykonawca zobowiązany jest uwzględnić w ofercie 50 godz. doradztwa wdrożeniowego. Zamawiający zobowiązuje się do zakupu co najmniej 20 godz. doradczych. Pozostała pula może być wykorzystana przez Zamawiającego w zależności od jego potrzeb.

VI. Ogólna charakterystyka Zamawiającego:

1. Zamawiający, jest jednostką sektora finansów publicznych – samorządu terytorialnego. Realizuje zadania publiczne wynikające z ustawy o samorządzie gminnym (Dz.U.2024.0.609)
2. Zamawiający realizuje zadania określone w part. 6 i art. 7 Ustawy o samorządzie gminnym.
3. Wszystkie informacje dotyczące Zamawiającego są dostępne na jego stronie internetowej.
4. Przybliżona liczba pracowników Zamawiającego to poniżej 200 osób.

ORGANIZACJA REALIZACJI OPISU PRZEDMIOTU ZAMÓWIENIA

1. Wykonawca wyznaczy, spośród ekspertów oddelegowanych do realizacji zamówienia Kierownika Projektu.



2. Kierownik projektu będzie posiadał pełną wiedzę o realizowanym projekcie oraz będzie odpowiedzialny za komunikację w projekcie i podpisywanie raportów częściowych z etapów realizacji prac, przedstawianie harmonogramów oraz ewentualnych zmian.
3. W ramach każdego etapu Wykonawca przeprowadzi przynajmniej jedno spotkanie inicjujące, na którym poinformuje w szczególności o harmonogramie pracy, sposobie realizacji, celach, produktach częściowych, kamieniach milowych.
4. W ramach etapów II-III Wykonawca powinien przewidzieć konsultacje w siedzibie Zamawiającego. W sytuacji wprowadzenia pracy zdalnej u Zamawiającego lub z innych ważnych przyczyn, Zamawiający dopuszcza by konsultacje i spotkania inicjujące kolejne etapy projektu realizowane były on-line za pomocą MS-Teams.
5. Wykonawca wymaga informowania w formie pisemnej o przebiegu realizacji prac z uwzględnieniem każdego etapu.
6. Każdy etap prac uznaje się za zakończony po przyjęciu przez obie strony raportu z zakończenia prac danego etapu.
7. Informacje, które będą przekazywane w celu realizacji niniejszego projektu, stanowią informacje chronione, w związku z tym realizacja projektu będzie wymagała akceptacji zapisów o zachowaniu poufności i zapewnieniu stosownej ochrony, w tym również dla danych osobowych.
8. Wszystkie dokumenty sporządzone będą w formie pisemnej w języku polskim, w formie papierowej oraz formie elektronicznej w formacie danych .pdf oraz jednym z formatów edytowalnych: .doc, .rtf, .xlsx.
9. Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.
10. Wykonawca w ramach 12 miesięcznej gwarancji, liczonej od dnia zakończenia ostatniego etapu, zobowiązany będzie do poprawy błędów w przekazanej dokumentacji niezależnie od jej formy wytworzenia, w terminie nie dłuższym niż 30 dni od daty zgłoszenia błędu przez Zamawiającego. Z uwagi na zapisy konkursowe Wykonawca oświadcza, że usługi gwarancyjne świadczone po dniu 31.12.2025 r. są usługami świadczonymi nieodpłatnie.