

Opis Przedmiotu Zamówienia

(zwany „OPZ”)

Usługa polegająca na przeglądzie, aktualizacji, opracowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji

I. Ogólne warunki realizacji zamówienia

1. Przedmiotem zamówienia jest opracowanie przez Wykonawcę dla Zamawiającego nowego systemu zarządzania bezpieczeństwem informacji, zwanego „**nowym SZBI**” oraz 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 do w terminie **do 180 dni kalendarzowych** licząc od dnia następnego po podpisaniu umowy.

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 własności 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:
 - a) dokument „Polityka Bezpieczeństwa Systemów Teleinformatycznych”, który opisuje wymagania i zasady bezpieczeństwa dla systemów teleinformatycznych,
 - b) 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 następujących zagadnień:
 - a) bezpieczeństwo zasobów ludzkich,
 - b) bezpieczeństwo fizyczne,
 - c) bezpieczeństwo cyberprzestrzeni,
 - d) bezpieczeństwo danych osobowych,
 - e) bezpieczeństwo informacji niejawnych,
 - f) obsługa incydentów,
 - g) zarządzanie ryzykiem,
 - h) użytkowanie systemów teleinformatycznych,
 - i) użytkowanie urządzeń mobilnych.
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 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. z 2024 r. poz. 773), 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 2024 r. poz. 1557, 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:
 - a) Polityka Bezpieczeństwa;
 - b) Organizacja bezpieczeństwa informacji;
 - c) Bezpieczeństwo zasobów ludzkich;
 - d) Zarządzanie aktywami;
 - e) Kontrola dostępu;
 - f) Kryptografia;
 - g) Bezpieczeństwo fizyczne i środowiskowe;
 - h) Bezpieczna eksploatacja;

- i) Bezpieczna komunikacja;
- j) Pozyskiwanie, rozwój i utrzymanie systemów;
- k) Relacje z dostawcami;
- l) Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- m) Aspekty bezpieczeństwa w zarządzaniu ciągłością działania;
- n) 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* (Dz. U. z 2024 r., poz. 1557 z późn. zm.)
- 5) ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz. U. z 2022 r., poz. 902 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 2024 r. poz. 1112);
- 7) ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2024 r. poz. 632 z późn. zm.);
- 8) ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2024 r., poz. 1077 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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148* (dyrektywa NIS 2)

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) kontrola dostępu,
 - f) bezpieczeństwo fizyczne i środowiskowe,
 - g) klasyfikacja informacji,
 - h) odpowiedzialność za zasoby,
 - i) postępowanie z nośnikami informacji,
 - j) użytkowanie urządzeń mobilnych i praca zdalna,
 - k) zarządzanie sprzętem informatycznym,
 - l) instalacja oprogramowania,
 - m) ochrona przed oprogramowaniem złośliwym,
 - n) kopie zapasowe,
 - o) zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
 - p) zarządzanie dokumentacją infrastruktury informatycznej,
 - q) monitorowanie systemów informatycznych,

- r) zarządzanie pojemnością,
 - s) serwis i konserwacja infrastruktury informatycznej,
 - t) zarządzanie podatnościami technicznymi,
 - u) zarządzanie incydentami bezpieczeństwa,
 - v) zabezpieczenia kryptograficzne,
 - w) bezpieczeństwo sieci i transmisji danych,
 - x) ochrona własności intelektualnej,
 - y) bezpieczeństwo informacji w relacjach z dostawcami,
 - z) ciągłość działania,
 - aa) zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
 - bb) weryfikacja zgodności z wymaganiami prawnymi,
 - cc) korzystanie z poczty elektronicznej i Internetu,
 - dd) zarządzanie usługami informatycznymi,
 - ee) utrzymanie i doskonalenie SZBI,
 - ff) 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 zależeć będzie od ich charakteru i każdorazowo należy do Zamawiającego.
3. Wykonawca zobowiązany jest uwzględnić w ofercie **40 godz.** doradztwa wdrożeniowego.

V. 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: **poniżej 40 osób**.
5. Liczba wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.), w tym:
 - a. Liczba komputerów (również przenośnych):
 - Komputery stacjonarne – 34 szt.
 - Laptopy - 5 szt.
 - b. Liczba serwerów (fizycznych, wirtualnych):
 - Serwery fizyczne centralne: 5 szt.
 - Serwery wirtualne: 8 szt.
 - c. Liczba pozostałych urządzeń podłączonych do sieci – 36 szt.
6. Liczba podsieci – 6 szt.
7. Liczba serwerowni – 1 szt.
8. Wdrożone Active Directory

VI. Organizacja realizacji 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 formy jej 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 zakończenia projektu przez Zamawiającego, są usługami świadczonymi nieodpłatnie.

Radłów 03.04.2025 r.

Zatwierdzono:

Marta Herduś

Zastępca Burmistrza Radłowa