**Załącznik nr 1 do ZO**

**Szczegółowy Opis Przedmiotu Zamówienia**

**Cyberbezpieczny Samorząd – wdrożenie SZBI**

# Zestawienie zakresu dostaw i usług

Zakres zamówienia obejmuje następujące elementy:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość** | **Jednostka miary** |
|  | Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz Polityki Bezpieczeństwa Informacji | 1 | usługa |

# Wymagania ogólne

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 cząstkowych z etapów realizacji prac, przedstawianie harmonogramów oraz ewentualnych zmian.
3. Wykonawca wymaga informowania w formie pisemnej o przebiegu realizacji prac z uwzględnieniem każdego etapu. Dopuszcza się wykorzystanie poczty elektronicznej.
4. 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.
5. Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.
6. 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 zakończenia projektu przez Zamawiającego, są usługami świadczonymi nieodpłatnie.

# Szczegółowy opis pozycji

## Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz Polityki Bezpieczeństwa Informacji

|  |
| --- |
| 1. Przedmiotem zamówienia jest analiza posiadanej obecnie przez Zamawiającego dokumentacji SZBI oraz opracowanie przez Wykonawcę dla Zamawiającego nowej dokumentacji / aktualizacja posiadanej dokumentacji systemu zarządzania bezpieczeństwem informacji, zwanego „**nowym SZBI**”. 2. Zakresem usługi objęty jest podmiot: Gmina Urzędów. 3. Zakres usługi obejmuje:    1. analizę działalności Zamawiającego;    2. aktualizację istniejącej dokumentacji SZBI lub opracowanie nowego SZBI wg oceny Wykonawcy i w uzgodnieniu z Zamawiającym.   **Analiza działalności Zamawiającego**   1. Analiza działalności Zamawiającego ma na celu identyfikację kontekstu SZBI. Analiza powinna objąć następujące zagadnienia: 2. obszary działalności Zamawiającego i realizowanych zadań; 3. strukturę organizacyjną Zamawiającego; 4. specyfikę pracy poszczególnych komórek organizacyjnych Zamawiającego; 5. systemy informatyczne użytkowane przez Zamawiającego; 6. rejestry publiczne pozostające we właściwości Zamawiającego; 7. SZBI aktualnie funkcjonujący u Zamawiającego; 8. wstępną identyfikację informacji przetwarzanych u Zamawiającego; 9. 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. 10. W celu przeprowadzenia analizy Zamawiający udostępni Wykonawcy niezbędne, posiadane dokumenty, w szczególności dotyczące aktualnie funkcjonującego SZBI.   **Aktualizacja / Opracowanie nowego SZBI**   1. Celem opracowania przez Wykonawcę wstępnej koncepcji SZBI, Zamawiający wskazuje poniżej ogólny ramowy zarys SZBI:   Określenie struktury dokumentacji 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:      1. dokument „Polityka Bezpieczeństwa Systemów Teleinformatycznych”, który opisuje wymagania i zasady bezpieczeństwa dla systemów teleinformatycznych,      2. 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:      1. bezpieczeństwo zasobów ludzkich,      2. bezpieczeństwo fizyczne,      3. bezpieczeństwo cyberprzestrzeni,      4. bezpieczeństwo danych osobowych,      5. bezpieczeństwo informacji niejawnych,      6. obsługa incydentów,      7. zarządzanie ryzykiem,      8. użytkowanie systemów teleinformatycznych,      9. użytkowanie urządzeń mobilnych.  1. Ramowy zarys SZBI, o którym mowa, 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. 2. 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. 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**”.   1. 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.   1. SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:    1. rozporządzenia KRI;    2. rozporządzeniaParlamentu 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 z późn. zm.);    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.   1. W ramach opracowania SZBI Wykonawca między innymi: 2. zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią sprawozdania zaakceptowanego przez Zamawiającego; 3. uwzględni w szczególności następujące zagadnienia:    * 1. określenie organizacji bezpieczeństwa informacji,      2. identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,      3. szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,      4. bezpieczeństwo w procesach zarządzania zasobami ludzkimi,      5. kontrola dostępu,      6. bezpieczeństwo fizyczne i środowiskowe,      7. klasyfikacja informacji,      8. odpowiedzialność za zasoby,      9. postępowanie z nośnikami informacji,      10. użytkowanie urządzeń mobilnych i praca zdalna,      11. zarządzanie sprzętem informatycznym,      12. instalacja oprogramowania,      13. ochrona przed oprogramowaniem złośliwym,      14. kopie zapasowe,      15. zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,      16. zarządzanie dokumentacją infrastruktury informatycznej,      17. monitorowanie systemów informatycznych,      18. zarządzanie pojemnością,      19. serwis i konserwacja infrastruktury informatycznej,      20. zarządzanie podatnościami technicznymi,      21. zarządzanie incydentami bezpieczeństwa,      22. zabezpieczenia kryptograficzne,      23. bezpieczeństwo sieci i transmisji danych,      24. ochrona własności intelektualnej,      25. bezpieczeństwo informacji w relacjach z dostawcami,      26. ciągłość działania,      27. zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,      28. weryfikacja zgodności z wymaganiami prawnymi,      29. korzystanie z poczty elektronicznej i Internetu,      30. zarządzanie usługami informatycznymi,      31. utrzymanie i doskonalenie SZBI,      32. przeprowadzanie audytów SZBI. 4. SZBI zostanie przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (.doc lub .docx). 5. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę 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.   **Produkty końcowe:** Wykonawca przekaże Zamawiającemu następujące produkty:   * Raport z audytu i analizy luk. * Kompletną, zatwierdzoną dokumentację SZBI w dwóch wersjach:   + Elektronicznej edytowalnej (np. w formacie \*.docx).   + Elektronicznej nieedytowalnej (w formacie \*.pdf), podpisanej kwalifikowanym podpisem elektronicznym przez osobę upoważnioną po stronie Wykonawcy.   **Współpraca:** Wykonawca będzie ściśle współpracował z wyznaczonym przez Zamawiającego przedstawicielem (np. Inspektorem Ochrony Danych, Administratorem Systemów Informatycznych).  **Odbiór:** Odbiór przedmiotu zamówienia nastąpi na podstawie protokołu zdawczo-odbiorczego podpisanego bez zastrzeżeń przez obie Strony po zrealizowaniu wszystkich zadań określonych w umowie. |