

Rzeczpospolita
PolskaDofinansowane przez
Unię Europejską

Opis przedmiotu zamówienia (OPZ) (charakterystyka i minimalne wymagania)

Przedmiot zamówienia: **Nowe systemy cyberbezpieczeństwa w Gminie Dzierżoń**

Element 2 – Zakup i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Przedmiotem zamówienia w zakresie części 2, jest podniesienie poziomu cyberbezpieczeństwa poprzez zakup i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), z uwzględnieniem potrzeb określonych w Ankiecie Dojrzałości Cyberbezpieczeństwa w JST. Realizacja zadania obejmuje kompleksowe wykonanie usługi, spełniającej poniższe wymagania:

Lp.	Element zadania	Ilość
I.	Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI	1 komplet
II.	Doradztwo w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa, outsourcing usług związanych z pełnieniem funkcji Koordynatora ds. KSC przez okres 24 miesięcy	1 pakiet

I. Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI - 1 komplet

Lp.	Zakres realizacji	Wymagania
1	Badanie aktualnej polityki bezpieczeństwa jako podstawowy element SZBI	Wymagane przeprowadzenie następujących czynności: 1) analiza wyników przeprowadzonego audytu wstępnego przez ekspertów; 2) wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Bezpieczeństwa Informacji; 3) doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 4) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki w obszarze przyjętej Polityki.
2	Polityka Zarządzania Systemem Teleinformatycznym	Wymagane przeprowadzenie następujących czynności: 1) analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2) wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Zarządzania Systemem Informatycznym; 3) doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 4) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące wszystkie procesy z obszaru Krajowych Ram Interoperacyjności.
3	Polityka Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT	Wymagane przeprowadzenie następujących czynności: 1) analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2) wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Zarządzania Ciągłością Działania;

		3) przygotowanie i przekazanie Polityki Zarządzania Ciągłością Działania wraz 4) z Planami Ciągłości Działania w obszarze IT; 5) doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 6) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące obszar utrzymania ciągłości działania.
4	Polityka Zarządzania Incydentami Cyberbezpieczeństwa	Wymagane przeprowadzenie następujących czynności: 1) analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2) wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Zarządzania Incydentami Cyberbezpieczeństwa; 3) przygotowanie i przekazanie Polityki Zarządzania Incydentami Cyberbezpieczeństwa; 4) przygotowanie i przekazanie Planu Reagowania na Incydenty; 5) przygotowanie i przekazanie Planu Zarządzania Podatnościami; 6) doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 7) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące wdrożoną Politykę Zarządzania Incydentami Cyberbezpieczeństwa oraz wymogów prawnych wynikających Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023r. poz. 913, 1703).
5	Polityka Ochrony Danych	Wymagane przeprowadzenie następujących czynności: 1) analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2) wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Ochrony Danych; 3) przygotowanie i przekazanie Polityki Ochrony Danych; 4) doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 5) przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące wdrożoną Politykę Ochrony Danych oraz omówienie przyjętych procedur zgodnie z przepisami z zakresu ochrony danych w oparciu o przepisy 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
6	Analiza Ryzyka Bezpieczeństwa Informacji	Wymagane przeprowadzenie następujących czynności: 1) analiza wyników przeprowadzonego audytu wstępnego przez ekspertów; 2) wizyta/wideokonferencja z przedstawicielem jednostki w celu przeprowadzenia analizy ryzyka; 3) przygotowanie i przekazanie Raportu z przeprowadzonej analizy ryzyka i omówienie obszarów o podniesionym ryzyku wraz z rekomendacjami ekspertów.

7	Wykonanie w ramach przeprowadzonych prac - aktualizacji, dostosowania i wdrożenia wskazanych procedur i dokumentów	<p>Wykaz procedur i dokumentów podlegających aktualizacji, dostosowaniu i wdrożeniu:</p> <ol style="list-style-type: none"> 1) procedury korzystania z urządzeń mobilnych, 2) procedury pracy zdalnej, 3) postępowanie z nośnikami, 4) procedury kontroli dostępu, 5) zabezpieczenie pomieszczeń i obiektów, 6) procedury czystego biurka, 7) procedury czystego ekranu, 8) procedury kopii zapasowych, 9) procedury ochrony logów, 10) bezpieczeństwo komunikacji, 11) zarządzanie bezpieczeństwem sieci, 12) przesyłanie informacji, 13) plany ciągłości działania, 14) procedury zarządzania incydentami, 15) prywatność i ochrona danych osobowych, 16) szacowanie ryzyka w obszarze bezpieczeństwa informacji, 17) szkolenia personelu, 18) plan zarządzania podatnościami, 19) plan reagowania na incydenty, 20) plan przywracania.
8	Wymagania inne	Zamawiający wymaga aby wykonawca w tworzonej SZBI ujął stan wynikający z wdrożenia systemu backupowego i wynikających z niego zmian.

II. Doradztwo w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa, outsourcing usług związanych z pełnieniem funkcji Koordynatora ds. KSC przez okres 24 miesiące – 1 pakiet

Lp.	Zakres realizacji	Wymagania
1	Zakres doradztwa	<ol style="list-style-type: none"> 1) Opracowanie procedury, w tym dokumentacji dotyczącej reagowania na incydenty. 2) Pełnienie funkcji osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wykonywania wobec tych podmiotów obowiązków. 3) Świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CDIRT. 4) Doradztwo w zakresie przekazanych zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa. 5) Przygotowywanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń.

		6) Sporządzenie informacji dotyczących prawnych zagadnień bezpieczeństwa informacji oraz cyberbezpieczeństwa. 7) Doradztwo w zarządzaniu incydentami oraz doradztwo w obsłudze incydentów. 8) Opracowanie i aktualizacja broszury pozwalającej na zrozumienie zagrożenia w obszarze cyberbezpieczeństwa i stosowania praktycznych sposobów zabezpieczania się przed tymi zagrożeniami w związku z realizacją zadań publicznych z wykorzystaniem systemów informacyjnych.
--	--	--

Usługi wdrożenia systemu SZBI – wymagania dodatkowe:

1. Zamawiający wymaga 24-miesięcznego świadczenia usługi doradztwa i utrzymania dokumentacji w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa.
2. Zamawiający oczekuje outsourcingu usług związanych z pełnieniem funkcji Koordynatora ds. KSC przez okres 24 miesięcy.
3. W ramach zadania Zamawiający wymaga cyklicznych spotkań 1 raz na kwartał, w celu realizacji postanowień wg ustalonego harmonogramu, natomiast w razie wystąpienia incydentu niezwłocznie po jego wystąpieniu, aż do całkowitego przywrócenia stanu poprzedzającego incydent.
4. Harmonogram spotkań zakłada 1-godzinne spotkanie zdalne celem omówienia stanu bieżącego, oszacowania ewentualnych ryzyk. Spotkania te będą miały formę zdalną i będą dotyczyły Zakresu doradztwa określonego w punktach 1 do 8.
5. Harmonogram 8 spotkań zostanie zrealizowany w terminach uzgodnionych z Zamawiającym, nie później niż w ostatnim tygodniu kończącym kwartał, począwszy od daty podpisania umowy. Data spotkania może ulec zmianie na pisemny wniosek Wykonawcy po uzyskanej zgodzie Zamawiającego.
6. W razie wystąpienia incydentu, Wykonawca zapewni jego obsługę do czasu ustania skutków i pełnego przywrócenia stanu poprzedzającego.