Załącznik nr 1 do umowy

(2.1) AKTUALIZACJA SZBI WRAZ Z AKTUALIZACJĄ POLITYKI ZARZĄDZANIA RYZYKAMI I SZKOLENIE PRACOWNIKÓW

Opis przedmiotu zamówienia (OPZ)

Przedmiotem zamówienia jest aktualizacja SZBI wraz z aktualizacją Polityki zarządzania ryzykiem i szansami w Urzędzie Miasta Bełchatowa.
Zamówienie realizowane przez Wykonawcę dotyczy aktualizacji istniejącego w Urzędzie rejestru ryzyk i SZBI **(Zamawiający nie dopuszcza utworzenia Polityki zarządzania ryzykiem i szansami i SZBI od podstaw lub na podstawie innego szablonu niż obowiązujący w Urzędzie).** W Urzędzie rejestr ryzyk funkcjonuje w ramach Kontroli zarządczej w tym Polityki zarządzania ryzykiem i szansami realizowanej w oparciu o funkcjonujący w Urzędzie System Zarządzania Jakością zgodny z normą ISO 9001.
Aktualizacja SZBI i rejestru ryzyk musi być zrealizowana z uwzględnieniem obowiązujących przepisów prawa w oparciu o przepisy 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 (KRI) w szczególności Rozdział 4 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz dobrych praktyk zawartych w innych dokumentach, w szczególności w poradniku grantu Cyberbezpieczny Samorząd.

Zamawiający wymaga, aby obecnie funkcjonujący SZBI oraz Polityka zarządzania ryzykiem i szansami w Urzędzie Miasta Bełchatowa zaktualizowane zostały pod kątem cyberbezpieczeństwa i bezpieczeństwa informacji, mając na uwadze poszczególne polityki, procedury, kompetencje i narzędzia do kontroli dostępu, obsługę incydentów w tym incydentów cyberbezpieczeństwa, polityki zarządzania podatnościami, procedury ciągłości działania Urzędu, opracowanie polityki bezpieczeństwa w relacji z dostawcami usług, stosowanie kryptografii i szyfrowania.
Zamawiający oczekuje analizy obowiązujących w Urzędzie formalnych i nieformalnych procedur i polityk, określenia ich adekwatności i skuteczności oraz wskazania zestawienia brakującej dokumentacji jako podstawy przygotowania do zaktualizowania dokumentacji SZBI i Polityki zarządzania ryzykiem i szansami.

Dokumentacja ma być zaktualizowana poprzez dodanie dodatkowych sekcji i procedur, celem ułatwienia zarządzania i przeglądu. **Format dokumentacji powinien obejmować wersje elektroniczne, zapewniające pełną dostępność i możliwość archiwizacji.**
Jeżeli Wykonawca uzna, że konieczne jest dołączenie dodatkowych dokumentów lub procedur, może je włączyć w ramach aktualizacji, aby jeszcze lepiej/precyzyjniej dostosować dokumentację do potrzeb Urzędu.
Dokumenty muszą zawierać kompleksową analizę kontekstu operacyjnego Urzędu, identyfikując wewnętrzne i zewnętrzne czynniki, które mogą wpłynąć na zarządzanie bezpieczeństwem informacji.

1. Zamawiający wymaga od Wykonawcy opracowania szczegółowego harmonogramu wdrożenia aktualizacji SZBI i Polityki zarządzania ryzykiem i szansami.
2. Harmonogram musi być zatwierdzony przez Zamawiającego przed rozpoczęciem implementacji.
3. Harmonogram wdrożenia aktualizacji musi zostać przedłożony Zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie Zamawiającego w celu lepszego dopasowania do warunków operacyjnych Zamawiającego.
4. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane Zamawiającemu i podlegają jego zatwierdzeniu.
5. Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu Zamawiającemu. Raporty powinny zawierać szczegółowe informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu.
6. Po pomyślnym zaktualizowaniu SZBI i Polityki zarządzania ryzykiem i szansami wymagane jest zatwierdzenie dokumentu przez Zamawiającego. Zatwierdzenie będzie udokumentowane na podstawie protokołu odbioru.

Zamawiający oczekuje ustalenia i uzgodnienia sposobu komunikacji w ramach realizacji przedmiotu zamówienia, który będzie gwarantował rozliczalność zadań aktualizacji SZBI i Polityki zarządzania ryzykiem i szansami u Zamawiającego przez wszystkie osoby zaangażowane w aktualizację. Zamawiający oczekuje uruchomienia platformy i używania jej w procesie zarządzania w tym wymiany informacji/pracy nad dokumentacją na czas realizacji przedmiotu zamówienia. Platformę w ramach tego zadania dostarcza Wykonawca. Platforma powinna posiadać jako minimum następujące funkcjonalności:

1. Tworzenie bazy pozwalającej na inwentaryzację aktywów.
2. Możliwość określenia analizy wpływu dla każdego składnika aktywów.
3. System zadaniowy, pozwalający na tworzenie i przypisywanie zadań poszczególnym pracownikom, rejestrujący realizację i zapewniający rozliczalność zadań, z możliwością tworzenia szablonów zadań.
4. Możliwość zarządzania, planowania i rozliczania pracy użytkowników i zespołów.
5. Rejestracja problemów i zmian.
6. Możliwość publikacji i edycji dokumentacji SZBI.
7. Przypisywanie użytkowników do grup.

Na spotkaniu wstępnym określony zostanie zakres prac, opracowany zostanie wstępny harmonogram i ukonstytuowanie zespołu wdrożeniowego, przeprowadzona zostanie analiza istniejących procesów polityk i procedur, wnioski z przeglądu istniejących polityk i procedur.
Cześć prac może być wykonana zdalnie. Zamawiający oczekuje **minimum 5 spotkań w Urzędzie**, na których w formie warsztatów zostaną przedstawione propozycje zmian do dokumentacji.

1. Propozycje przypisania ról w SZBI.
2. Określenie i wyjaśnienie roli najwyższego kierownictwa w szczególności wytyczanie kierunków, monitoring i kontrola SZBI.

Spotkania powinny być zaplanowane na ok **4 godziny** i powinny zawierać krótkie szkolenie przedstawiające omawiany temat z punktu widzenia SZBI oraz warsztaty, na których wspólnie przedstawiciele Urzędu oraz Wykonawca wypracują wnioski do dalszych etapów aktualizacji SZBI i Polityki zarządzania ryzykiem i szansami.
Wszystkie opracowane polityki, procedury, procesy muszą zostać skutecznie wdrożone w Urzędzie.

AKTUALIZACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Cel etapu

Zarządzanie bezpieczeństwem informacji w jednostce to zadanie wymagające przygotowania i wdrożenia zestawu regulacji wewnętrznych adekwatnych do ryzyka wymagań prawnych i organizacyjnych.

Szczegółowy opis etapu

Zamawiający oczekuje aktualizacji i o ile zajdzie taka potrzeba przygotowania uzupełnienia formalnej dokumentacji, która zawierać będzie zadania i obowiązki regulujące postępowanie pracowników, zapewniając zachowanie odpowiedniego poziomu bezpieczeństwa informacji.
W toku tego działania Wykonawca zaktualizuje lub przygotuje wszystkie niezbędne (wymagane dobrymi praktykami oraz obowiązującymi przepisami prawa) polityki, schematy organizacyjne, regulaminy, procedury i instrukcje, procesy oraz nadrzędną wobec nich – politykę bezpieczeństwa informacji (PBI). W rozumieniu tego zadania (PBI) to podstawowy zestaw dokumentów, który odgrywa kluczową rolę w zarządzaniu bezpieczeństwem.
Każdy dokument (regulacja wew.) musi zostać zaakceptowany przez zespół wdrożeniowy jako praktycznie funkcjonujący w Urzędzie.
Dla każdego dokumentu mogą być wskazane mierniki pozwalające na ocenę skuteczności oraz sposób monitorowania osiągania celów (adekwatność i skuteczność).
PBI powinno definiować cele oraz zakres SZBI, a także zawierać deklarację wsparcia zarządzania bezpieczeństwem przez kierownictwo Urzędu.
Dokumentację SZBI należy opracować w odniesieniu do zadań Zamawiającego, z uwzględnieniem obszarów, których dotyczy oraz możliwości prezentowania poszczególnych dokumentów różnym grupom odbiorców.

Opis kontekstu zewnętrznego i wewnętrznego

Opis kontekstu jest niezbędny do przeprowadzenia oceny ryzyka i wdrożenia procesu zarządzania ryzykiem.
Zamawiający wymaga wsparcia ze strony Wykonawcy w przygotowaniu dokumentu opisującego kontekst Zamawiającego.

Inwentaryzacja aktywów

Zamawiający oczekuje, że Wykonawca pokieruje zespołem wdrożeniowym Zamawiającego podczas przygotowania inwentaryzacji aktywów związanych z bezpieczeństwem informacji i cyberbezpieczeństwem. Inwentaryzacja aktywów może być zrealizowana za pomocą oprogramowania, którym dysponuje Zamawiający lub innym.

Inwentaryzacja aktywów powinna być przygotowana w oparciu o „procesy, procedury, instrukcje, zadania", uzupełnione o aktywa informatyczne, niezbędne do realizacji tego zadania. W wyniku działania zespołu wdrożeniowego podczas inwentaryzacji aktywów musi zostać jednoznacznie wskazany właściciel (składnika aktywów, procesu, informacji i elementów infrastruktury IT wspierających ten proces).
Etap ten wymaga wsparcia ze strony Wykonawcy dla właścicieli poszczególnych zabezpieczeń SZBI i opisanych w PBI w ich uruchomieniu, monitorowaniu i raportowaniu.

Ciągłość działania
Należy opracować Plan(-y) Ciągłości Działania w Urzędzie w zakresie zapewnienia ciągłości działania aktywów informacyjnych.
Plan ciągłości działania powinien w szczególności zawierać:
1. Określenie przedmiotu planu oraz zakresu stosowania.
2. Ramy czasowe oraz poziom wznowienia działania.
3. Określenie odpowiedzialności i uprawnień.
4. Określenie planu i zasad przeprowadzania szkoleń dla uczestników planu.
5. Określenie zasad aktualizacji planu.
6. Określenie wzoru protokołu z testów ciągłości działania.
7. Określenie procedury postępowania:
    1) warunki uruchomienia planu,
    2) osoby wymagane do realizacji planu,
    3) zasoby wymagane do realizacji planu,
    4) opis działań oraz osoby odpowiedzialne za realizację planu,
    5) określenie zasad przeprowadzania testów ciągłości działania systemów informatycznych.

Wdrożenie polityk i procedur
Wszystkie opracowane polityki, procedury, procesy wraz z miernikami muszą zostać skutecznie wdrożone w Urzędzie tak by stały się częścią kultury organizacyjnej i były stosowane w codziennej pracy.
Zamawiający wymaga wsparcia ze strony Wykonawcy w procesie wdrożenia.
Względem funkcjonującego SZBI w Urzędzie Wykonawca opracuje procedury na bazie obecnie obowiązujących w Urzędzie. Struktura dokumentacji powinna być jasna i zrozumiała dla wszystkich użytkowników SZBI w Urzędzie.

Sposób prowadzenia wdrożenia ciągłości działania i inwentaryzacji aktywów
Część prac na tym etapie może być wykonana zdalnie. Zamawiający **oczekuje minimum 5 spotkań w Urzędzie**, na których w formie warsztatów zostaną przedstawione następujące zagadnienia.
1. Spotkanie wstępne określające zakres prac i wstępny harmonogram inwentaryzacji aktywów dla wszystkich zaangażowanych stron.
2. Określenie i wyjaśnienie roli najwyższego kierownictwa i właścicieli poszczególnych procesów (usług i zadań) w Planie Ciągłości Działania Systemów Informatycznych.
3. Warsztaty I - Plan Ciągłości Działania Systemów Informatycznych na wypadek katastrofy.

Spotkania 1-3 powinny być zaplanowane na ok 4h i powinny zawierać krótkie szkolenie przedstawiające omawiany temat z punktu widzenia SZBI oraz warsztaty, na których

wspólnie przedstawiciele Urzędu oraz konsultanci wypracują elementy niezbędne do realizacji tego zadania.

Przegląd zarządzania

Przegląd zarządzania jest kluczowym elementem SZBI. Regularne przeprowadzanie przeglądów pozwala na ciągłe doskonalenie systemu i zapewnienie skutecznej ochrony informacji w Urzędzie.

Na tym etapie Zamawiający oczekuje wsparcia przez Wykonawcę przy przeprowadzeniu przeglądu zarządzania, podsumowującego funkcjonowanie całego systemu. Zamawiający oczekuje od Wykonawcy przygotowania zakresu i harmonogramu przeglądu zarządzania oraz wszystkich niezbędnych wzorów raportów.

Przegląd zarządzania to systematyczna ocena skuteczności SZBI w Urzędzie. Ma on na celu zweryfikowanie, czy SZBI działa zgodnie z założeniami, czy system ten jest skuteczny w ochronie informacji w Urzędzie.

Celem przeglądu jest:

- Ocena skuteczności SZBI: Sprawdzenie czy system działa zgodnie z politykami i procedurami, czy osiąga zakładane cele.
- Identyfikacja obszarów wymagających poprawy: Wskazanie miejsc, w których system może być udoskonalony, aby zwiększyć jego efektywność.
- Weryfikacja oceny ryzyka z uwzględnieniem nowych zagrożeń dla bezpieczeństwa informacji i weryfikacja oceny, czy istniejące zabezpieczenia są wystarczające.
- Zaproponowanie działań korygujących: Opracowanie planu działań, które mają na celu usunięcie zidentyfikowanych nieprawidłowości i zapobieganie ich powtórzeniu.
- Zapewnienie ciągłego doskonalenia SZBI: Gwarantowanie, że system jest stale dostosowywany do zmieniających się warunków i wymagań.

Ramowy zakres przeglądu powinien obejmować:

- sprawdzenie, na jakim etapie są zadania i poprawki ustalone podczas wcześniejszych ocen SZBI,
- identyfikację nowych zagrożeń, zmian w technologii, przepisach prawnych czy w strukturze Urzędu, które mogą wpłynąć na bezpieczeństwo informacji,
- analizę oczekiwań klientów, pracowników i innych stron zainteresowanych, które mają interes w tym, aby informacje były bezpieczne,
- pozyskanie informacji zwrotnej dotyczącej skuteczności zabezpieczeń, w tym:
    - trendy w niezgodnościach i działaniach korygujących,
    - wyniki monitorowania i pomiarów,
    - podsumowanie wyników zewnętrznych lub wewnętrznych kontroli/audytów systemu bezpieczeństwa,
    - spełnianiu celów w zakresie bezpieczeństwa informacji,
    - zebranie opinii od różnych grup na temat skuteczności zabezpieczeń,
    - podsumowanie oceny ryzyka i analizy potencjalnych zagrożeń i działań podjętych, aby je zminimalizować,
    - ocena świadomości pracowników: sprawdzenie czy pracownicy są świadomi zasad bezpieczeństwa informacji i stosują się do nich,
    - ocena, jak były zarządzane incydenty bezpieczeństwa, jakie wnioski z nich wyciągnięto i jakie działania zostały podjęte, aby zapobiec podobnym sytuacjom w przyszłości,

- ocena efektywności komunikacji w zakresie bezpieczeństwa informacji.

Cześć prac na tym etapie może być wykonana zdalnie. Zamawiający **oczekuje minimum 3 spotkań w Urzędzie**, na których w formie warsztatów zostaną przedstawione następujące zagadnienia.

1. Spotkanie wstępne określające zakres prac i wstępny harmonogram przeglądu zarządzania dla wszystkich zaangażowanych stron, określenie i wyjaśnienie roli najwyższego kierownictwa w przeglądzie zarzadzania.
2. Wsparcie zespołu wdrożeniowego przy przygotowaniu sprawozdania na przegląd zarządzania, wsparcie najwyższego kierownictwa przy podsumowaniu przeglądu zarzadzania.
3. Podsumowanie aktualizacji SZBI dla całego zespołu wdrożeniowego

Spotkania powinny być zaplanowane na ok 4h i powinny zawierać krótkie szkolenie przedstawiające omawiany temat z punktu widzenia SZBI oraz warsztaty, na których wspólnie przedstawiciele urzędu oraz konsultanci wypracują elementy przeglądu zarządzania.

POLITYKA ZARZĄDZANIA RYZYKIEM I SZANSAMI

Konieczność aktualizacji Polityki zarządzania ryzykiem i szansami w Urzędzie wynika z potrzeby systematycznego podejścia do identyfikacji, oceny i zarządzania ryzykiem w obszarze cyberbezpieczeństwa i bezpieczeństwa informacji w odniesieniu do zadań realizowanych przez Urząd. Aktualizacja rejestru ryzyk stanowi kluczowy element w procesie aktualizacji SZBI, co pozwoli na lepsze zrozumienie, monitorowanie i minimalizowanie ryzyk, a także zwiększenie odporności organizacyjnej na incydenty bezpieczeństwa. Aktualizacja ryzyka ma zapewnić spełnianie wymogów 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 oraz art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

W ramach wdrożenia procesu zarządzania ryzykiem oczekujemy przygotowania przez Wykonawcę procesu zarzadzania ryzykiem wg. Następującego schematu:

1. **Diagnozy stanu obecnego:**

Przeprowadzenie audytu obecnego stanu zarządzania ryzykiem w Urzędzie. Identyfikacja mocnych i słabych stron, obszarów do poprawy. Analiza dokumentacji, procedur i systemów. Wywiady z kluczowymi pracownikami.

2. **Aktualizacja polityki i strategii zarządzania ryzykiem:**

Aktualizacja Polityki zarządzania ryzykiem i szansami (metodyki), określającej cele, zasady i ramy działania. Zdefiniowanie ryzyka i tolerancji na ryzyko. Ustalenie ról i odpowiedzialności w procesie zarządzania ryzykiem. Aktualizacja procedur identyfikacji, analizy, oceny i monitorowania ryzyka.
Wykonawca zaktualizuje procedurę zarządzania ryzykiem uwzględniając międzynarodowe standardy w zakresie cyberbezpieczeństwa, jak również normę ISO, na której opiera się obecnie procedura zarządzania ryzykiem. Powyższe muszą obejmować ciągłe doskonalenie metod zarządzania ryzykiem, aby zapewnić ich aktualność i skuteczność.
Realizacja zamówienia wymaga zastosowania narzędzi (arkuszy kalkulacyjnych), które wspomogą procesy identyfikacji, analizy oraz zarządzania ryzykiem:

1) Wykonawca wykorzysta obecnie funkcjonujące w Urzędzie i dostarczy Zamawiającemu arkusze kalkulacyjne do zarządzania ryzykiem, które umożliwią systematyczne śledzenie, analizę ryzyk.

Wykonawca musi przeprowadzić proces identyfikacji nowych zagrożeń i ryzyk, które mogły pojawić się od czasu ostatniej aktualizacji rejestru (np. przy zmianie planu pracy (wykreślenie/dodanie zadania). Proces ten musi obejmować analizę zmian w otoczeniu zewnętrznym i wewnętrznym Urzędu, a także uwzględnienie nowych technologii, procesów operacyjnych i zmian w przepisach prawnych, które mogą wpłynąć na poziom ryzyka.

3. **Identyfikacja i analiza ryzyka:**

Przeprowadzenie warsztatów z udziałem pracowników w celu identyfikacji potencjalnych ryzyk. Analiza ryzyka z wykorzystaniem metod jakościowych i ilościowych. Identyfikacja potencjalnych zagrożeń, które mogą wpływać na integralność, dostępność lub poufność informacji. Ocena ryzyka, czyli prawdopodobieństwa wystąpienia zagrożeń oraz konsekwencji, jakie mogą one mieć dla integralności, dostępności lub poufności informacji. Przydzielanie ryzyka do kategorii, np. wysokie, średnie lub niskie, aby lepiej zrozumieć priorytety i skalę zagrożeń zgodnie z przyjętą metodyką. Ocena prawdopodobieństwa wystąpienia i potencjalnych skutków ryzyka. Klasyfikacja ryzyka według poziomu istotności. Ewentualna aktualizacja obecnie funkcjonującego arkusza (excel) oceny ryzyka.

4. **Aktualizacja planu reagowania na ryzyko:**

Opracowanie strategii reagowania na ryzyko dla każdego zidentyfikowanego zagrożenia. Wdrożenie działań prewencyjnych i kontrolnych. Opracowanie planów awaryjnych i procedur postępowania w sytuacjach kryzysowych poprzez powiązanie z procesem zachowania ciągłości działania. Opracowanie planu postępowania z ryzykiem na podstawie wyników analizy ryzyka, określającego konkretne kroki prowadzące do minimalizacji ryzyka. Wprowadzenie odpowiednich kontroli, procedur i zabezpieczeń, które będą chronić informacje i zapewnią ich integralność, dostępność i poufność.

5. **Wdrożenie systemu oraz monitorowanie i raportowanie:**

Wsparcie przy wdrażaniu środków ochrony i upewnienie się, że środki te są zgodne z wynikami analizy ryzyka oraz przyczynią się do minimalizacji ryzyka utraty integralności, dostępności lub poufności informacji. Wdrożenie systemu monitorowania ryzyka i skuteczności wdrożonych działań. Opracowanie systemu raportowania najwyższemu kierownictwu Urzędu. Przygotowanie harmonogramu regularnych, okresowych przeglądów analizy ryzyka w celu sprawdzenia, czy istnieją nowe zagrożenia lub zmiany, które mogą wymagać aktualizacji planu działania. Monitorowanie środowiska i wprowadzanie niezbędnych zmian dla utrzymania lub podniesienia poziomu bezpieczeństwa informacji o ryzyku dla kierownictwa. Wprowadzenie wskaźników monitorowania ryzyka (KRI). Przygotowanie harmonogramu regularnych, okresowych przeglądów analizy ryzyka w celu sprawdzenia, czy istnieją nowe zagrożenia lub zmiany, które mogą wymagać aktualizacji planu działania oraz monitorowania środowiska i wprowadzania niezbędnych zmian dla utrzymania lub podniesienia poziomu bezpieczeństwa informacji.

6. **Szkolenia i wsparcie:**

Przeprowadzenie warsztatów dla pracowników zaangażowanych w proces zarządzania ryzykiem. Wsparcie w bieżącym zarządzaniu ryzykiem oraz zapewnienie pracownikom odpowiedniej wiedzy, celem podwyższenia ich świadomości na temat postępowania w

przypadku wystąpienia takich zagrożeń. Edukowanie na temat istniejących procedur i postępowań, które minimalizują ryzyko.

Integracja
Na tym etapie Zamawiający oczekuje od Wykonawcy analizy innych istniejących w Urzędzie procesów zarządzania. Przygotowanie integracji procesu zarządzania ryzykiem z istniejącymi w Urzędzie procesami zarządczymi. Opracowanie odpowiednich harmonogramów i zakresów.
Cześć prac na tym etapie może być wykonana zdalnie. Zamawiający oczekuje **minimum 4 spotkań** w siedzibie Zamawiającego, na których, w formie warsztatów, zostaną przedstawione następujące zagadnienia.

1. Spotkanie wstępne określające zakres prac i wstępny harmonogram procesu zarządzania ryzykiem dla wszystkich zaangażowanych stron.
2. Określenie i wyjaśnienie roli najwyższego kierownictwa i właścicieli poszczególnych procesów (usług i zadań) w procesie zarządzania ryzykiem.
3. Warsztaty I – Identyfikacja, analiza i ocena ryzyka.
4. Warsztaty II - Postępowanie z ryzykiem, poziomy ryzyka.

Spotkania 1-4 powinny być zaplanowane na ok 4h i powinny zawierać krótkie szkolenie przedstawiające omawiany temat z punktu widzenia SZBI oraz warsztaty, na których wspólnie przedstawiciele Urzędu oraz konsultanci wypracują elementy niezbędne do realizacji tego zadania.

SZKOLENIE

1. **Wykonawca przeszkoli pracowników Urzędu** z zaktualizowanego i zatwierdzonego przez Zamawiającego SZBI i z Polityki zarządzania ryzykiem i szansami. Wykonawca jest zobowiązany zapewnić, aby szkolenie pokrywało kluczowe obszary takie jak, procedury operacyjne i reagowania na incydenty, zarządzanie ryzykiem, wdrożone i zaktualizowane polityki a także prawne i regulacyjne aspekty ochrony danych i cyberbezpieczeństwa. Szkolenie powinno również skupić się na umiejętnościach praktycznych, takich jak właściwe postępowanie w przypadku wykrycia zagrożeń dla bezpieczeństwa informacji, cyberzagrożeń oraz na rozwijaniu świadomości i kultury bezpieczeństwa wśród pracowników.
2. Zamawiający podkreśla znaczenie szkolenia jako integralnej części procesu wdrażania zaktualizowanego SZBI oraz Polityki zarządzania ryzykiem i szansami mającego na celu nie tylko zwiększenie kompetencji pracowników, ale także poprawę ogólnego poziomu bezpieczeństwa informacji w Urzędzie. **Wykonawca musi więc zaprojektować program szkolenia**, który jest interaktywny i dostosowany do różnych poziomów wiedzy uczestników, aby maksymalizować jego efektywność i zapewnić, żeby wszystkie cele szkoleniowe zostały osiągnięte. Materiały te muszą być zaprojektowane w sposób umożliwiający łatwe zrozumienie i przyswajanie wiedzy przez uczestników o różnym poziomie zaawansowania oraz różnych potrzebach. Materiały powinny również zawierać praktyczne wskazówki dotyczące wdrażania polityk i procedur w życie codzienne Urzędu, uwzględniając specyfikę i potrzeby Urzędu oraz promując praktyki zapewniające równość i niedyskryminację.

3. **Wykonawca musi zaprojektować i opracować szczegółowy program szkolenia, który następnie musi zostać przedstawiony Zamawiającemu do zatwierdzenia. Program ten musi być dostosowany do potrzeb Urzędu, zgodnie z wymogami dotyczącymi SZBI oraz procedury zarządzania ryzykiem.**
4. Wykonawca opracuje harmonogram szkolenia, który uwzględni czas trwania szkolenia, daty, czas na pytania i odpowiedzi uczestników szkolenia oraz na interaktywne dyskusje, czas na przerwy, aby umożliwić im wyjaśnienie wszelkich wątpliwości.
5. Po opracowaniu programu szkolenia, Wykonawca przedstawi go Zamawiającemu do akceptacji. Zamawiający przeprowadzi przegląd programu, aby upewnić się, że spełnia on wszystkie wymagane standardy oraz adekwatnie adresuje potrzeby i specyfikę Urzędu, a w razie potrzeby Zamawiający może zaproponować zmiany lub uzupełnienia, które zostaną omówione i wdrożone przez Wykonawcę przed ostatecznym zatwierdzeniem programu.
6. Wykonawca przeprowadzi szkolenie stacjonarnie w siedzibie Zamawiającego, w grupach po maksymalnie **50 osób (kolejno po sobie lub rozłożone w ciągu 14 dni) x 4 godziny zajęć, dzień (jedna/dwie grupy). Jednostką czasową szkolenia jest 1 godzina zegarowa, przewiduje się dwie przerwy trwające po 15 minut w ciągu dnia,** łączna liczba osób do przeszkolenia wynosi **230 (liczba osób może ulec zmianie o +/- 10% osób)**.
   W przypadku szkoleń zdalnych grupy mogą być liczniejsze, wymaga to dodatkowych ustaleń z Zamawiającym.
7. Zamawiający wymaga, aby treści szkoleniowe były zróżnicowane w zależności od roli uczestników:
   1) **Dla zwykłych użytkowników** – program szkolenia skupi się na podstawowych aspektach SZBI oraz zarządzaniu ryzykami, w tym na zrozumieniu polityk bezpieczeństwa, zasadach postępowania w przypadku zauważenia potencjalnego zagrożenia w wykonywaniu codziennych zadań.
   2) **Dla kadry kierowniczej** – szkolenie będzie zawierało rozszerzone moduły dotyczące zarządzania ryzykiem, strategii odpowiedzi na incydenty bezpieczeństwa oraz zaawansowanych aspektów tworzenia i utrzymania polityk bezpieczeństwa, nadzoru nad bezpieczeństwem informacji.
8. Zamawiający dopuszcza możliwość przeprowadzenia szkolenia w formie zdalnej. Wykonawca jest zobowiązany do zapewnienia odpowiedniego narzędzia do zdalnego połączenia, które umożliwi efektywne i interaktywne przekazywanie wiedzy oraz aktywne uczestnictwo pracowników w szkoleniu. Narzędzie to musi umożliwiać prowadzenie transmisji wideo, współdzielenie ekranu, interaktywne dyskusje w czasie rzeczywistym.

(2.2) USŁUGA PRZEPROWADZENIA AUDYTU KRI I USŁUGA PRZEPROWADZENIA AUDYTU PODATNOŚCI

Opis przedmiotu zamówienia (OPZ)

Przedmiotem zamówienia jest przeprowadzenie audytu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o przepisy 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 (KRI) w szczególności Rozdział 4 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. **Przeprowadzenie trzech audytów KRI (jeden w roku 2024, drugi w roku 2025, trzeci w roku 2026) i trzech audytów podatności (jeden w roku 2024, drugi w roku 2025, trzeci w roku 2026).** Przygotowany w wyniku audytu raport będzie zawierał opis sytuacji aktualnej, dowody potwierdzające zgodność oraz wskazywać obszary, w których nie ma zgodności z wymaganiami oraz zalecenia dotyczące tych obszarów. Zamawiający oczekuje omówienia wyników audytu na spotkaniu z przedstawicielami kierownictwa Urzędu w siedzibie Zamawiającego (wykluczona forma zdalna).

Zamawiający oczekuje, że Wykonawca posiada doświadczenie w realizacji podobnych zadań i może się wykazać odpowiednimi referencjami i certyfikatami.

1) Zamawiający wymaga od Wykonawcy opracowania szczegółowego harmonogramu przeprowadzenia audytów.
2) Harmonogram musi być zatwierdzony przez Zamawiającego przed rozpoczęciem audytów.
3) Harmonogram musi zostać przedłożony Zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie Zamawiającego w celu lepszego dopasowania do warunków operacyjnych Zamawiającego.
4) Wykonawca jest zobowiązany do regularnego przeglądu i aktualizacji harmonogramu w odpowiedzi na zmieniające się otoczenie i zmiany organizacyjne realizacji zadania lub na wniosek Zamawiającego. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane Zamawiającemu i podlegają jego zatwierdzeniu.
5) Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu Zamawiającemu. Raporty powinny zawierać szczegółowe informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu.

Audyt KRI zostanie przeprowadzony w siedzibie Zamawiającego **(nie dopuszcza się realizacji w sposób zdalny).**

Testy zostaną zrealizowane zgodnie z międzynarodową metodologią NIST, PTES, OWASP w aktualnie obowiązującej wersji. Zidentyfikowane ryzyka zostaną sklasyfikowane w oparciu o kryteria Common Vulnerability Scoring System, które umożliwiają precyzyjne, liczbowe opisanie ryzyka zidentyfikowanej podatności. Zamawiający wymaga, aby wszystkie testy podatności były przeprowadzane w sposób ręczny, przy wykorzystaniu automatycznych narzędzi jedynie na tych etapach, gdzie automatyzacja podstawowych prac pozwoli zaoszczędzić czas i przekierować go na działanie z jednoznaczną korzyścią

dla Zamawiającego. Przedstawiony raport z przeprowadzonych prac będzie zawierał minimum:

a) Metrykę testu - zawierającą informacje o zespole wykonującym test, dacie testu, dacie sporządzenia raportu.
b) Ujęcie wniosków strategicznych w podsumowaniu zarządczym raportu.
c) Cel i zakres testów.
d) Przyjęcie modelu klasyfikacji ryzyka.
e) Metodologię oraz narzędzia.
f) Szczegółowy opis podatności wraz z rekomendacjami ich usunięcia.

Zamawiający wymaga, aby testy podatności były prowadzone w sposób hybrydowy. **Minimum 2 dni robocze** w siedzibie Zamawiającego.
Scenariusz zostanie opracowany i przygotowany z uwzględnieniem systemów i usług wykorzystywanych przez zamawiającego i potwierdzony z zespołem IT u Zamawiającego. Zamawiający nie dopuszcza, aby scenariusz testów był narzucony przez Wykonawcę (z puli odgórnie ustalonych scenariuszy).
Działania zostaną zakończone szczegółowym raportem z przeprowadzonych testów z podsumowaniem dla kierownictwa Zamawiającego.