

Załącznik nr 1 do Zaproszenia

Załącznik nr 2 do Umowy

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

### I. Nazwa zadania:

**Audyt i dostosowanie wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Prudniku i jednostkach organizacyjnych Powiatu Prudnickiego.**

### II. Informacje podstawowe:

#### **Przedmiot zamówienia:**

Audyt wdrożeniowy Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Prudniku, Domu Pomocy Społecznej w Prudniku, Poradni Psychologiczno - Pedagogicznej w Prudniku oraz Powiatowym Centrum Pomocy Rodzinie w Prudniku.

Aktualizacja i dostosowanie Systemu Zarządzania Bezpieczeństwem Informacji do obowiązujących przepisów prawa, w tym PN EN ISO 27001:2023 w szczególności w zakresie procesów zarządzania ryzykiem i cyberbezpieczeństwa, z uwzględnieniem zakupionego sprzętu i licencji.

Zadanie realizowane w ramach projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-IP.01-001/23 Fundusze Europejskie na rozwój cyfrowy 2021-2027 Priorytet II: Zaawansowane usługi cyfrowe działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Umowa o powierzenie grantu FERC.02.02-C5.01-001/23/0460 FERC.02.02.C5.01-001/23/2024

#### **Miejsce świadczenia usługi:**

- 1) Starostwo Powiatowe w Prudniku, ul. Kościuszki 76, 48-200 Prudnik, woj. opolskie,
- 2) Powiatowe Centrum Pomocy Rodzinie w Prudniku, ul. Kościuszki 55a, 48-200 Prudnik, woj. Opolskie;
- 3) Poradnia Psychologiczno - Pedagogiczna w Prudniku, ul. Parkowa 10, 48 – 200



Prudnik, woj. Opolskie;

- 4) Dom Pomocy Społecznej w Prudniku, ul. Młyńska 11, 48 – 200 Prudnik, woj. Opolskie.

**Czas trwania umowy:** 8 m-cy od dnia zawarcia umowy

**Wymagania wobec Wykonawcy:**

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia określony w opisie przedmiotu zamówienia tj.:

- 1) w ciągu ostatnich 3 lat zrealizował co najmniej trzy audyty dotyczących bezpieczeństwa informacji w podmiocie realizującym zadania publiczne;
- 2) w okresie ostatnich 3 lat zrealizował co najmniej 2 projekty polegające na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów realizujących zadania publiczne;
- 3) w okresie ostatnich 3 lat wykonał co najmniej 1 audyt cyberbezpieczeństwa połączony z testami penetracyjnymi w podmiocie realizujących zadania publiczne,
- 4) posiada zespół składający się, z co najmniej 2 osób, w tym:
  - a) co najmniej 1 osobę posiadającą wiedzę i doświadczenie w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji zgodnie z normą PN EN ISO 27001, potwierdzone ważnym certyfikatem ukończenia przedmiot zamówienia, w tym zakresie lub innym równoważnym dokumentem;
  - b) co najmniej 1 osobę posiadającą aktualne uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie certyfikatów uprawniających do przeprowadzenia audytu;
- 5) nie realizował usług lub dostaw na rzecz zamawiającego w ramach realizowanego projektu Cyberbezpieczny Samorząd.

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do:

- współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek do sporządzonej dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia;
- zapewnienia dostępności dla osób ze szczególnymi potrzebami.

### **Wymogi dodatkowe:**

- W okresie ostatnich 3 lat Wykonawca zrealizował co najmniej 4 audyty cyberbezpieczeństwa w podmiocie realizującym zadania publiczne, potwierdzone referencjami – Zamawiający na etapie oceny ofert przyzna dodatkowe 10 pkt.
- W okresie ostatnich 3 lat Wykonawca zrealizował co najmniej 3 projekty polegające na świadczeniu usług w zakresie stworzenia dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów realizującym zadania publiczne, potwierdzone referencjami - Zamawiający na etapie oceny ofert przyzna dodatkowe 10 pkt.
- W okresie ostatnich 3 lat Wykonawca wykonał co najmniej 2 audyty cyberbezpieczeństwa połączone z testami penetracyjnymi w podmiocie realizującym zadania publiczne, potwierdzone referencjami- Zamawiający na etapie oceny ofert przyzna dodatkowe 10 pkt.

### **Wymagane dokumenty:**

- Wykonawca składa poprawnie wypełniony formularz oferty;
- Wykonawca wraz z ofertą przedłoży portfolio z którego wynika, że przeprowadził większą lub wymaganą przez Zamawiającego ilość audytów zawierające takie dane jak:
  - a) nazwy podmiotów, na rzecz których przedmiot zamówienia był realizowany,
  - b) daty realizacji przedmiotu zamówienia,
  - c) tematy przedmiotu zamówienia,
  - d) Imienia i Nazwiska osób, które te przedmiot zamówienia realizowały,
- certyfikaty Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001;
- certyfikaty wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;

### **Informacje Zamawiającego:**

- Zamawiający zastrzega sobie prawo do wzywania do wyjaśnień Wykonawców w celu potwierdzenia referencji osób oraz przedmiotu zamówienia bezpośrednio w podmiotach, na rzecz których Wykonawca przedmiot zamówienia realizował,

- Zamawiający zastrzega sobie prawo do wzywania do wyjaśnień Wykonawców w celu potwierdzenia referencji osób oraz przedmiotu zamówienia bezpośrednio poprzez przedłożenie referencji imiennych dla osób, które zostaną wskazane do realizacji przedmiotu zamówienia, wystawionych przez podmioty, u których wskazana osoba realizowała przedmiot zamówienia,

### **III. Informacje szczegółowe:**

#### **1. AUDYT WDROŻENIOWY:**

Kryteriami audytu są:

- Rozporządzenie 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;
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma ISO/IEC 27001;
- Norma PN-EN ISO/IEC 22301.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- wypełnionych przez Wykonawcę 4 „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)”, wg załącznika numer 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”, odrębnie dla każdej jednostki;
- rekomendacji do wdrożenia w celu poprawy bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa Zamawiającego;
- raportu na zakończenie realizacji przedmiotu zamówienia.

#### **Audyt musi obejmować weryfikację:**

- 1) systemu zarządzania bezpieczeństwem informacji,
- 2) zapewnienia aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
- 3) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
- 4) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,

- 5) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
- 6) zapewnienia realizacji przedmiotu umowy przy udziale osób zaangażowanych w proces przetwarzania informacji,
- 7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- 8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- 9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
- 10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- 11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
- 12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
- 13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- 14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

W ramach audytu Wykonawca zobowiązany jest do przeprowadzenia co najmniej 8 testów penetracyjnych (min. 2 w każdej jednostce) i sporządzenia raportów skanu podatności razem z oceną ryzyka znalezionych zagrożeń oraz określone zalecenia pozwalające na ich eliminację lub minimalizację ryzyka.

Testy penetracyjne powinny składać się z min. następujących elementów:

- 1) test zewnętrzny,
- 2) test sieci wewnętrznej,
- 3) testy słabości ludzkich (czyli wszystkie chywy dozwolone). Podawanie się za inne osoby tak by zbadać słabości użytkowników czy dadzą się podejść by uzyskać hasła lub zainstalować niechciane oprogramowanie.

Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 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 akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 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) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem.

Zamawiający nie dopuszcza prowadzenia konsultacji, audytów i analiz stanu istniejącego i określenia stanu faktycznego zabezpieczeń technicznych, w formule zdalnej poza siedzibą Zamawiającego lub jednostek podległych, z wyjątkiem testów penetracyjnych.

Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzelementowej skali:

- 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone,
- 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników),
- 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle

zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

## 2. AKTUALIZACJA I DOSTOSOWANIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI:

W oparciu o przeprowadzony audyt i diagnozę dojrzałości systemu cyberbezpieczeństwa Wykonawca zobowiązany jest do opracowania, wdrożenia i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, w tym m.in. aktualizacja polityki bezpieczeństwa, analizy ryzyka (w tym opracowanie i wdrożenie metodyk) w zakresie wymaganych procedur. Celem usługi w ramach działania będzie aktualizacja i wdrożenie procedur systemu zarządzania bezpieczeństwem informacji wdrożonych u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostek. Analiza zostanie przeprowadzona zgodnie z wymogami ISO/IEC 19011:2002 oraz 19011:2018.

W efekcie zostanie zaktualizowana także polityka bezpieczeństwa w zakresie ochrony danych osobowych. Usługa obejmuje również aktualizację dokumentów opisujących zbiory danych i ich zgodność z wymogami prawnymi oraz aktualizację dokumentów opisujących miejsca i sposoby przetwarzania danych osobowych.

Na usługę aktualizacji i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się co najmniej:

1. Wykonanie oceny obecnej dostępnej dokumentacji.
2. Określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych poprzez przeprowadzenie audytu zabezpieczeń dostępu do danych oraz przygotowanie raportu wraz z zaleceniami i projektem zmian spełnienie wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych.
3. Przeprowadzenie instruktażu wprowadzającego dla pracowników w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka.

4. Aktualizacja/opracowanie Polityki Bezpieczeństwa zgodnej z wymaganiami normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych w zakresie:

- 1) organizacja systemu bezpieczeństwa informacji;
- 2) zarządzanie aktywami;
- 3) zarządzanie zasobami ludzkimi;
- 4) organizacja bezpieczeństwa fizycznego i środowiskowego;
- 5) zarządzanie komunikacją i eksploatacją;
- 6) rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania;
- 7) kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
- 8) akwizycja, rozwój i utrzymanie systemu;
- 9) zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- 10) zarządzanie ciągłością działania;
- 11) zarządzania kopiami zapasowymi;
- 12) zarządzania monitoringiem;
- 13) zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
- 14) używania urządzeń komputerowych;
- 15) metoda szacowania i postępowania z ryzykiem;
- 16) deklaracja stosowania SZBI.

5. Poprzez wdrożenie SZBI należy rozumieć także aktualizację/utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego lub jednostek podległych, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego lub jednostek podległych oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Ponadto:

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

- 1) opracowania/zaktualizowania procedur bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne;
- 2) opracowania/zaktualizowania zasad odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo;
- 3) opracowania/zaktualizowania polityki szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego ich prowadzenia.
- 4) opracowania/zaktualizowania treści zarządzenia wdrażającego SZBI dla Zamawiającego i w jednostkach podległych;
- 5) opracowania/zaktualizowania planu postępowania z ryzykiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika;
- 6) opracowania/zaktualizowania szczegółowego sposobu realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
- 7) opracowania/zaktualizowania procedury wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki;
- 8) opracowania/zaktualizowania polityki szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych;
- 9) opracowania/zaktualizowania kluczowych aktywów informacyjnych Jednostek (zbiory danych/systemy/usługi);
- 10) opracowania/zaktualizowania rejestru ryzyk uwzględniający aktywa Jednostki;
- 11) opracowania/zaktualizowania zagrożeń związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem;
- 12) opracowania/zaktualizowania planu postępowania z ryzykiem związanym z zagrożeniami bezpieczeństwa informacji;
- 13) opracowania/zaktualizowania kompleksowej polityki zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków, identyfikowane, ustanawiane i oceniane ryzyka, priorytetyzacji odpowiedzi na ryzyka oraz system oceny ryzyka;
- 14) opracowania/zaktualizowania kompleksowej polityki zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych;

- 15) opracowania/zaktualizowania planu zarządzania podatnościami, uwzględniający obowiązek dokumentowania ryzyka z nimi związanego;
- 16) opracowania/zaktualizowania kompleksowej polityki zarządzania zapisami zdarzeń / logów/ inspekcji;
- 17) opracowania/zaktualizowania polityki użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych;
- 18) opracowania/zaktualizowania kompleksowej polityki reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów, ustalenia sposobu reagowania na incydenty uwzględniające procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
- 19) opracowania/zaktualizowania polityki planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.

Wykonawca zobowiązany jest do wprowadzania zmian opracowanej dokumentacji, o ile okaże się to konieczne w związku ze zmianami regulacji prawnych lub w związku ze zmianami organizacyjnymi lub technicznymi Zamawiającego i jednostek podległych.

#### **IV. Etapy realizacji przedmiotu zamówienia:**

Etap I. Audyt zerowy.

1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenie spełnienia wymagań i zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych.
3. Inwentaryzacja aktywów informacyjnych i ocena ryzyka.
4. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
5. Analiza dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analiza dokumentacji Polityki Bezpieczeństwa Danych Osobowych.
7. Zestaw działań mających na celu określenie stanu faktycznego zabezpieczeń technicznych w systemie informatycznym:
  - 1) ocena schematu sieci,

- 2) określenie rodzaju połączeń,
- 3) określenie segmentów sieci,
- 4) przeprowadzenie oceny środowiska informatycznego,
- 5) ocena sposobu identyfikowania i logowania użytkowników,
- 6) analiza zarządzania kontami użytkowników,
- 7) analiza strony www i BIP pod kątem ochrony danych osobowych,
- 8) analiza systemu backupów i archiwizacji danych,
- 9) określenie miejsc redundancji w sieci i systemach informatycznych,
- 10) analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach,
- 11) analiza konfiguracji zabezpieczeń baz danych,
- 12) określenie bezpieczeństwa aplikacji i serwerów www,
- 13) analiza konfiguracji urządzeń sieciowych: switchy, routery, ids, ips, utm, firewall,
- 14) ocena zabezpieczeń dostępu do sieci publicznej, w tym testy penetracyjne),
- 15) badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania,
- 16) analiza zabezpieczeń stacji roboczych,
- 17) analiza ochrony danych na komputerach przenośnych,
- 18) badanie zabezpieczeń nośników zewnętrznych,
- 19) sprawdzenie procedur zarządzania ciągłością działania systemów informatycznych.

8. Opracowanie raportu z audytu zerowego zawierającego analizę bezpieczeństwa i adekwatności zabezpieczeń stosowanych przez Zamawiającego w odniesieniu do sieci i systemów informatycznych oraz rodzaju danych w nich przetwarzanych, z uwzględnieniem obowiązujących przepisów prawa, zasad wiedzy technicznej, wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych.

Etap II. Zastosowanie zabezpieczeń na podstawie zaleceń poaudytowych.

1. Konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego;
2. Konsultacje przy wdrożeniu zabezpieczeń organizacyjnych – polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami itp.

### Etap III. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1. Przeprowadzenie instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji.

2. Zakres SZBI:

- 1) określenie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
- 2) określenie zasięgu organizacji;
- 3) badanie środowiska zewnętrznego, powiązań z innymi organizacjami, systemami oraz dostawcami.

3. Zdefiniowanie wymaganych polityk SZBI:

- 1) uwzględnienie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
- 2) analiza wymagań prawnych oraz wymagań wynikających z umów;
- 3) uwzględnienie sposobu ustalania celów oraz wyznaczania kierunków działań w ramach systemu.

4. Szacowanie ryzyka:

- 1) wybór metody szacowania ryzyka;
- 2) określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
- 3) zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.

5. Wybór celów zabezpieczeń:

- 1) zdefiniowanie celów zabezpieczeń na podstawie listy zawartej w załączniku A normy PN- EN ISO/IEC 27001:2023;
- 2) zdefiniowanie własnych celów zabezpieczania i zabezpieczeń;
- 3) uwzględnienie wyników procesu szacowania ryzyka i określenie postępowania z ryzykiem;
- 4) określenie środków ochrony.

### Etap IV. Inwentaryzacja i szacowanie ryzyka SZBI.

1. Przeprowadzenie instruktażu dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych.

2. Wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych.

### 3. Zdefiniowanie planu postępowania z ryzykiem:

- 1) przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
  - 2) szacowanie i ocena ryzyka – zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
  - 3) zdefiniowanie planu postępowania z ryzykiem;
  - 4) określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
  - 5) określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.
- ### 4. Opracowanie raportu z oceny ryzyka.

## Etap V. Opracowanie niezbędnej dokumentacji SZBI.

### 1. Opracowanie wspólnie z pracownikami Zamawiającego lub jednostek podległych wymaganych procedur i instrukcji:

- 1) opracowanie Polityki Bezpieczeństwa Informacji;
  - 2) opracowanie Polityki Ochrony Danych Osobowych;
  - 3) opracowanie Instrukcji Zarządzania Systemem Informatycznym;
  - 4) opracowanie procedur i instrukcji wymaganych przez normę PN-EN ISO/IEC 27001:2023 oraz KRI;
  - 5) opracowanie procedur i instrukcji dopasowanych do specyfiki działalności organizacji;
  - 5) opracowanie Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa;
  - 6) opracowanie procedury audytu wewnętrznego;
  - 7) opracowanie procedury nadzoru nad dokumentacją;
  - 8) opracowanie procedury działań korygujących i zapobiegawczych;
  - 9) opracowanie procedury zachowania ciągłości działania;
  - 10) opracowanie planów ciągłości działania.
- ### 2. Wykonanie projektu zabezpieczeń - opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
- ### 3. Opracowanie programu uświadamiania i szkoleń.
- ### 4. Przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji.

5. Przeprowadzenie instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji.

Etap VI. Weryfikacja i monitorowanie SZBI.

1. Przeprowadzenie wraz z pracownikami organizacji audytu wewnętrznego.
2. Opracowanie raportu z audytu wewnętrznego.
3. Przeprowadzenie wraz z pracownikami organizacji przeglądu systemu SZBI:
  - 1) przegląd zagrożeń;
  - 2) przegląd podatności;
  - 3) określenie i weryfikacja ryzyk;
  - 4) weryfikacja planu postępowania z ryzykiem;
  - 5) sprawdzenie zabezpieczeń i celów zabezpieczeń;
  - 6) określenie zgodności zakresu SZBI;
  - 7) weryfikacja zgodności z politykami i celami zabezpieczeń;
  - 8) przegląd i ocena skuteczności zabezpieczeń;
  - 9) weryfikacja zgodności wykorzystywania procedur;
  - 10) weryfikacja zgodności obowiązków i uprawnień w ramach SZBI;
  - 11) analiza audytów bezpieczeństwa;
  - 12) weryfikacja dokumentacji i sposobu postępowania z incydentami;
  - 13) weryfikacja sugestii oraz informacji zwrotnych od zainteresowanych stron;
  - 14) sprawdzenie aktualności procedur ciągłości działania.
4. Opracowanie raportu końcowego zgodnie z wymogami konkursu grantowego.

#### **V. Informacje końcowe:**

Przedmiot zamówienia musi zostać przeprowadzony w zakresie spełniającym wymagania określone w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd”, opublikowany na stronie Centrum Projektów Polska Cyfrowa pod adresem: <http://www.gov.pl/cppc/cyberbezpieczny-samorząd>.