

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Część 3 pn.: Przeprowadzenie „Diagnozy cyberbezpieczeństwa”, opracowanie oraz wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa

1. Przeprowadzenie „Diagnozy cyberbezpieczeństwa”

1. W ramach przedmiotu zamówienia należy przeprowadzić audyt oraz wykonać diagnozę cyberbezpieczeństwa dla Urzędu Gminy w Sierpcu zgodnie z wymaganiami programu „Cyfrowa Gmina” oraz obowiązującymi przepisami prawa w tym zakresie.

Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina.

Regulamin Konkursu Grantowego Cyfrowa Gmina wraz z formularzem - załącznikiem nr 8 został zamieszczony na stronie Centrum Projektów Polska Cyfrowa <https://www.gov.pl/web/cppc/cyfrowa-gmina>.

2. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwane Rozporządzeniem KRI).
3. Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
4. Dokument końcowy musi być podpisany przez osobę posiadającą uprawnienia (wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) raport oraz wypełniony formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina) należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

2. Opracowanie oraz wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Celem usługi w ramach działania będzie aktualizacja procedur zarządzania bezpieczeństwem informacji wdrożonych w Gminie Giżycko z uwzględnieniem uwarunkowań i specyfiki niniejszego projektu oraz specyfiki jednostki. Analiza zostanie przeprowadzona zgodnie z wymogami ISO/IEC 19011:2002. W efekcie zostanie zaktualizowana 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 opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się:

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 ISO/IEC 27001 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. Opracowanie Polityki Bezpieczeństwa zgodnej z wymaganiami normy PN ISO/IEC 27001 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
5. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Poszczególne etapy realizacji usługi.

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-ISO/IEC 27001 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) Przeprowadzenie oceny środowiska informatycznego.
 - 4) Ocena sposobu identyfikowania i logowania użytkowników.
 - 5) Analiza zarządzania kontami użytkowników.
 - 6) Analiza strony www i BIP pod kątem ochrony danych osobowych.
 - 7) Analiza systemu backupów i archiwizacji danych.
 - 8) Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
 - 9) Analiza konfiguracji zabezpieczeń baz danych.
 - 10) Analiza konfiguracji urządzeń sieciowych: switchy, UTM.
 - 11) Ocena zabezpieczeń dostępu do sieci publicznej.
 - 12) Analiza zabezpieczeń stacji roboczych.
 - 13) Analiza ochrony danych na komputerach przenośnych.
 - 14) Badanie zabezpieczeń nośników zewnętrznych.
 - 15) Sprawdzenie procedur zarządzania ciągłością działania.
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-ISO/IEC 27001 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 ISO/IEC 27001;
 - 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 instruktaży 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 wymaganych procedur i instrukcji:
 - 1) opracowanie Polityki Bezpieczeństwa Informacji;
 - 2) opracowanie Instrukcji Zarządzania Systemem Informatycznym;
 - 3) opracowanie procedur i instrukcji wymaganych przez normę PN ISO/IEC 27001;
 - 4) 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 wraz z pracownikami zamawiającego 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 szkolenia.
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 z przeglądu.

Zamawiający zastrzega, że opracowanie dokumentacji SZBI powinno rozpocząć się w ciągu 7 dni od wezwania Wykonawcy do realizacji zakresu zadań opisanego w niniejszym punkcie.

Zamawiający żąda udzielenia gwarancji na opracowanie dokumentacji SZBI na okres minimum 24 miesięcy:

1. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do usunięcia wszelkich nieprawidłowości (błędów) w opracowanej dokumentacji SZBI zidentyfikowanych po terminie odbioru dokumentacji. Usunięcie nieprawidłowości (błędów) w opracowanej dokumentacji nastąpi w terminie nie dłuższym niż 14 dni od dnia zgłoszenia przez Zamawiającego nieprawidłowości (błędów) pisemnie bądź za pomocą poczty elektronicznej.
2. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do dostosowania i aktualizacji opracowanej dokumentacji SZBI do zmian środowiska Zamawiającego oraz wymagań prawnych w terminie nie dłuższym niż 14 dni od dnia przekazania przez Zamawiającego zgłoszenia. Zamawiający dokonuje zgłoszenia, o którym mowa w niniejszym ustępie drogą pisemną bądź za pomocą poczty elektronicznej.

3. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do dostarczania poprawionej dokumentacji SZBI, dostosowania i aktualizacji opracowanej dokumentacji SZBI do zmian środowiska Zamawiającego oraz wymagań prawnych.

Pozostałe informacje:

• Liczba pracowników -	30
• Ilość lokalizacji:	1
• Ilość serwerów fizycznych	2
• Ilość stacji roboczych	29
• Ilość urządzeń sieciowych:	5
• Ilość pozostałych urządzeń podłączonych do sieci:	6
• Ilość podsieci:	1
• Ilość serwerowni:	1
• Ilość adresów zewnętrznych:	1
• wdrożony Active Directory:	Nie

3. Przeprowadzenie szkolenia w zakresie cyberbezpieczeństwa,

dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczenia danych.

Wymagania dotyczące organizacji szkolenia:

- szkolenie odbędzie się w siedzibie Zamawiającego w trybie stacjonarnym oraz na platformie e-learningowej w trybie zdalnym,
- W szkoleniu będzie brało udział ok. 30 osób - 3 grupy szkoleniowych,
- ilość godzin w trybie stacjonarnym dla każdej grupy wyniesie 5.
- szkolenie będzie prowadzone w języku polskim,
- Wykonawca zapewni materiały szkoleniowe, w odpowiedni sposób oznakowane,
- każdy uczestnik szkolenia otrzyma zaświadczenie/certyfikat o ukończeniu szkolenia,
- Wykonawca zapewni kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia.
- Wykonawca zobowiązany jest do przekazania dokumentacji szkolenia Zamawiającemu w formie papierowej (dokumentacja fotograficzna w formie elektronicznej).
- Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym koszty swojego ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanu dokumentów. Wyżywienie podczas szkolenia każdy uczestnik zapewnia sobie we własnym zakresie.

Zakres szkolenia:

- 1) cyberbezpieczeństwo - dlaczego jest ważne, jaki jest cel szkolenia uświadamiającego, kto jest zobowiązany do ochrony fizycznego oraz cyfrowego mienia firmy, kim jest hacker, cele ataków,
- 2) narzędzia ataków.

- 3) bezpieczeństwo danych i kont: co to są dane, poufność, dostępność, integralność podstawowe pojęcia (uwierzytelnienie, autoryzacja, uprawnienia konta, uwierzytelnianie wieloskładnikowe), role bezpieczeństwa w organizacji, cykl życia danych, konta użytkowników - najlepsze praktyki
- 4) hasła: - najlepsze praktyki, zarządzanie hasłami, uwierzytelnienie wieloskładnikowe, najczęściej używane hasła,
- 5) bezpieczeństwo sieci oraz urządzeń mobilnych: wprowadzenie do sieci komputerowych, zagrożenia w sieciach komputerowych,
- 6) malware: co to jest malware, różne rodzaje malware, wektory ataku, sygnały skutecznego ataku, jak się zabezpieczyć,
- 7) inżynieria społeczna: jaka jest najlepsza ochrona przed tego typu atakami, techniki ataków socjotechnicznych,
- 8) przykłady ataków.
- 9) Inne zagadnienia, które Wykonawca uzna za ważne do przekazania osobom szkolonym w zakresie cyberbezpieczeństwa

Wykonawca jest zobowiązany po ukończeniu szkolenia do wydania każdemu uczestnikowi zaświadczeń/certyfikatów potwierdzających ukończenie szkolenia z logotypami identyfikującymi projekt i informacją, że projekt jest wspierany przez program operacyjny i finansowany przez UE z danego funduszu oraz dostarczyć Zamawiającemu kopie wydanych zaświadczeń/certyfikatów.