

Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Wińsko w ramach projektu pn. „Gmina Wińsko - Cyberbezpieczny Samorząd”

1. Przedmiotem zamówienia jest usługa opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Wińsko w ramach projektu pn. „Gmina Wińsko - Cyberbezpieczny Samorząd”
2. Podmioty objęte przedmiotem zamówienia
 - Urząd Gminy Wińsko
adres: pl. Wolności 2, 56-160 Wińsko,
 - Pomieszczenie biurowe w Filii Żłobka Wyspa Skarbów – Wińsko
adres: ul. Szkolna 4, 56-160 Wińsko.
 - Pomieszczenie biurowe w Gminny punkt konsultacyjno-informacyjny programu „czyste powietrze”–Wińsko
adres: Kościuszki 5/1A, 56-160 Wińsko.
 - Pomieszczenie biurowe w Gminny Ośrodek Pomocy Społecznej– Wińsko
adres: pl. Wolności 13, 56-160 Wińsko.
3. Zadanie objęte jest dofinansowaniem w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”.
4. Zakres realizacji usługi obejmuje opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301. Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:
 - 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),
 - ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.),
 - 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. 2024 poz. 773).

Wykonawca zobowiązany jest do wytworzenia dokumentacji, formularzy, opracowania zasad postępowania, procedur, itd., które będą zgodne z zapisami Regulaminu Konkursu Grantowego oraz Wzorem Umowy o powierzeniu Grantu dostępnych na stronie:

<https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad>

I. Ogólny zakres zadań Wykonawcy:

ETAP I

1. Wykonanie audytu wstępnego obejmującego min.:
 - inwentaryzację uprawnień w programach i systemach informatycznych,
 - inwentaryzację aktywów,
 - rozpoznanie struktury organizacyjnej i realizowanych procesów oraz wymagań prawnych funkcjonowania jednostki.
2. Stworzenie/aktualizacja dokumentacji SZBI z uwzględnieniem istniejących procedur.
3. Opracowanie zasad i formularzy dotyczących nadawania i odbierania uprawnień w programach informatycznych.

ETAP II

4. Aktywny udział w inwentaryzacji aktywów oraz przypisaniu własności aktywów.
5. Analiza ryzyka i opracowanie planu postępowania z ryzykiem.
6. Dostosowanie procedur do istniejącego ryzyka.
7. Opracowanie planu ciągłości działania.

ETAP III

8. Przeprowadzenie stacjonarnego szkolenia dla kadry kierowniczej i pracowników z zakresu funkcjonowania i stosowania SZBI.
9. Opracowanie działań korygujących i zapobiegawczych.
10. Przygotowanie harmonogramu przeglądów funkcjonowania SZBI.

II. Wymagania stawiane wykonawcy:

Wykonawca musi dysponować i przeznaczyć do realizacji zamówienia co najmniej jedną osobę będącą audytorem posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) oraz posiadającą doświadczenie zawodowe w zakresie audytowania systemów zarządzania bezpieczeństwem informacji (SZBI).

Kompletną dokumentację SZBI wraz formularzami, opracowaniami zasad postępowania, procedur oraz nową Politykę Ochrony Danych Osobowych należy sporządzić w 2 egzemplarzach w wersji papierowej oraz 1 egz. w wersji elektronicznej, edytowalnej.

III. Sposób realizacji zadania:

1. **Zamawiający wymaga aby wszystkie prace związane z przeprowadzaniem wywiadów, ankiet i analiz wśród pracowników Zamawiającego realizowane były przez przedstawiciela Wykonawcy w siedzibie Zamawiającego; Zamawiający wyklucza możliwość stosowania ankiet do samodzielnego wypełnienia przez pracowników Zamawiającego.**
2. **Wykonawca zobowiązany jest do stawiennictwa w siedzibie Zamawiającego na każde jego żądanie związane z realizacją przedmiotu zamówienia.**

IV. Wymagania dotyczące Polityki Bezpieczeństwa Informacji:

Zamawiający wymaga aby wdrożona Polityka Bezpieczeństwa Informacji w sposób usystematyzowany oraz jednoznaczny opisywała i regulowała wymienione niżej zagadnienia oraz

obszary funkcjonowania wynikające bezpośrednio z celów stosowania zabezpieczeń stanowiących załącznik A do normy ISO/IEC 27001.

Polityka Bezpieczeństwa Informacji (zagadnienia ogólne):

- znaczenie bezpieczeństwa informacji dla organizacji
- cele jakie organizacja zamierza osiągnąć w zakresie bezpieczeństwa informacji,
- obszar stosowania polityki,
- zgodność z obowiązującymi przepisami i normami.

Organizacja bezpieczeństwa informacji:

- role i odpowiedzialność za bezpieczeństwo informacji,
- rozdzielanie obowiązków,
- bezpieczeństwo informacji w zarządzaniu projektami,
- polityka stosowania urządzeń mobilnych,
- telepraca.

Bezpieczeństwo zasobów ludzkich:

- postępowanie sprawdzające przed zatrudnieniem,
- warunki zatrudnienia,
- odpowiedzialność kierownictwa,
- uświadamianie i szkolenia z zakresu bezpieczeństwa informacji
- zakończenie zatrudnienia i zmiana zakresu obowiązków.

Zarządzanie aktywami:

- inwentaryzacja aktywów,
- własność aktywów,
- akceptowalne użycie aktywów,
- zwrot aktywów,
- klasyfikowanie informacji
- oznaczanie informacji
- postępowanie z aktywami,
- zarządzanie nośnikami wymiennymi,
- wycofywanie nośników,
- przekazywanie nośników.

Kontrola dostępu:

- polityka kontroli dostępu,
- dostęp do sieci i usług sieciowych,
- rejestrowanie i wyrejestrowanie użytkowników,
- przydzielanie dostępu użytkownikom,
- zarządzanie prawami uprzywilejowanego dostępu (w tym zasady funkcjonowania administratorów podstawowych, takich jak np.: admin, administrator, root),
- przegląd praw dostępu użytkowników,
- odbieranie lub dostosowanie praw dostępu,
- stosowanie poufnych informacji uwierzytelniających,
- ograniczanie dostępu do informacji.
- procedury bezpiecznego logowania,
- system zarządzania hasłami,
- użycie uprzywilejowanych programów narzędziowych,
- kontrola dostępu do kodów źródłowych programów,

Kryptografia:

- polityka stosowania zabezpieczeń kryptograficznych,
- zarządzanie kluczami.

Bezpieczeństwo fizyczne i środowiskowe.

- fizyczna granica obszaru bezpiecznego,
- fizyczne zabezpieczenie wejść,
- zabezpieczenie biur, pomieszczeń i obiektów,
- ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
- praca w obszarach bezpiecznych,
- obszary dostaw i załadunku,
- lokalizacja i ochrona sprzętu,
- systemy wspomagające,
- bezpieczeństwo okablowania,
- konserwacja sprzętu,
- wynoszenie aktywów,
- bezpieczeństwo sprzętu i aktywów poza siedzibą,
- bezpieczne zbywanie lub przekazywanie do ponownego użycia
- pozostawienie sprzętu użytkownika bez opieki,
- polityka czystego biurka i czystego ekranu.

Bezpieczna eksploatacja:

- dokumentowanie procedur eksploatacyjnych,
- zarządzanie zmianami,
- zarządzanie pojemnością,
- zabezpieczenia przed szkodliwym oprogramowaniem,
- kopie zapasowe,
- rejestrowanie zdarzeń,
- ochrona informacji w dziennikach zdarzeń,
- rejestrowanie działań administratorów i operatorów,
- synchronizacja zegarów,
- instalacja oprogramowania w systemach produkcyjnych,
- zarządzanie podatnościami technicznymi,
- ograniczenia w instalowaniu oprogramowania.

Bezpieczeństwo komunikacji:

- zabezpieczenia sieci,
- bezpieczeństwo usług sieciowych,
- rozdzielanie sieci,
- polityki i procedury przesyłania informacji,
- wiadomości elektroniczne.

Pozyskiwanie, rozwój i utrzymanie systemów:

- analiza i specyfikacja wymagań bezpieczeństwa informacji,
- zabezpieczanie usług aplikacyjnych w sieciach publicznych,
- procedury kontroli zmian w systemach.

Analiza ryzyka:

- strategia zarządzania ryzykiem - opis konkretnych działań odnoszących się do zarządzania ryzykiem, w tym: opis procesu, narzędzia i techniki, role i zakresy odpowiedzialności, skala

oceny prawdopodobieństwa i wpływu ryzyka, progi tolerancji na ryzyko, kategorie ryzyka,

- szablony (wzory dokumentów) niezbędne w zarządzaniu ryzykiem, kluczowe wskaźniki efektywności i wskaźniki wczesnego ostrzegania, harmonogram działań, raportowanie,
- diagnoza ryzyka - identyfikacja ryzyk pozwalająca ocenić sytuację i zdarzenia pod kątem ich możliwego wpływu na bezpieczeństwo informacji,
- analiza i ocena - analiza ryzyka (ocena) z wykorzystaniem metody oceny jakościowej/iłościowej, monitorowanie ryzyka,
- rejestr ryzyk.

Plan ciągłości działania:

- identyfikacja kluczowych zasobów, procesów, usług i dostawców,
- scenariusze utraty ciągłości działania,
- zasady komunikacji w sytuacjach kryzysowych,
- plany przywracania ciągłości działania,
- redundancja zasobów i usług kluczowych,
- zasady testowania planu.

V. Ochrona danych osobowych

Zamawiający wymaga aby zagadnienia związane z ochroną danych osobowych opracowane były w wydzielonym dokumencie (Polityka Ochrony Danych Osobowych). Zamawiający wymaga aby dokument ten zawierał w szczególności:

- struktura organizacji ochrony danych osobowych,
- zasady przekazywania danych odbiorcom (zasady powierzenia i udostępnienia danych),
- zasady privacy by design oraz privacy by default,
- zasady retencji danych osobowych,
- procedura szkoleń oraz nadawania upoważnień do przetwarzania danych,
- procedura postępowania z incydentami związanymi z ochroną danych osobowych,
- procedura oceny skutków dla ochrony danych osobowych (DPIA),
- procedura realizacji praw osób, których dane dotyczą,
- procedura audytu zgodności przetwarzania danych osobowych,
- opis organizacyjnych środków bezpieczeństwa,
- opis fizycznych środków bezpieczeństwa,
- opis technicznych środków bezpieczeństwa,
- wzory ewentualnych formularzy do powyższych zasad i procedur.

VI. Wymagania dotyczące polityki bezpieczeństwa systemu informatycznego

Zamawiający wymaga aby wszystkie zagadnienia odnoszące się bezpośrednio do systemu informatycznego opracowane były w wydzielonym dokumencie do zapisów którego odnosić się będą zarówno Polityka Bezpieczeństwa Informacji oraz Polityka Ochrony Danych Osobowych. Zamawiający wymaga aby dokument ten regulował następujący (minimalny) zakres działań/zagadnień:

- nadawanie uprawnień użytkownikom systemów informatycznych należących do Zamawiającego w sposób precyzyjny i jednoznaczny, umożliwiające wykonywanie okresowej kontroli uprawnień w programach i systemach informatycznych,
- zasady nadawania uprawnień uprzywilejowanych (ASI),
- nadawanie uprawnień w systemach informatycznych niepodlegających nadzorowi ze strony administratora lokalnego (np. ZUS PUE, GUS, ePUAP),

- organizacja certyfikatów SSL,
- organizacja kluczy szyfrujących,
- zasady użytkowania zewnętrznych nośników informacji,
- zasady użytkowania komputerów mobilnych,
- zasady wykonywania pracy zdalnej przez pracowników Zamawiającego,
- zasady nawiązywania połączeń zdalnych przez wsparcie techniczne producentów programów (w trybie nadzorowanym i nienadzorowanym),
- zasady nawiązywania połączeń zdalnych przez Administratorów Systemu Informatycznego,
- archiwizacja danych i testowanie kopii bezpieczeństwa,
- kontrola dostępu do sieci, systemu i aplikacji,
- użytkowanie i zabezpieczenia stanowiska użytkownika,
- bezpieczeństwo fizyczne i środowiskowe,
- kontrola połączeń z siecią publiczną,
- zasady wykorzystania zabezpieczeń kryptograficznych,
- aktualizacja i testowanie oprogramowania.

Dokumentacja opisująca zasady funkcjonowania i kontroli systemu informatycznego powinna zawierać szablony wszystkich wykazów i rejestrów które powinny być prowadzone przez użytkowników lub administratorów systemu informatycznego.

VII. Wymagania dotyczące zakresu szkoleń dla kadry kierowniczej i pracowników z zakresu funkcjonowania i stosowania SZBI

Szkolenie prowadzone dla pracowników Urzędu powinno obejmować m.in.:

- Wymogi wynikające z Krajowych Ram Interoperacyjności (KRI), Ustawa o krajowym systemie cyberbezpieczeństwa (UoKSC) i Ogólne rozporządzenie o ochronie danych (RODO)
- zarządzanie ryzykiem w bezpieczeństwie informacji
- System Zarządzania Bezpieczeństwem informacji – jak skutecznie przestrzegać procedur wdrożonej Polityki Bezpieczeństwa Informacji.
- Ciągłość działania – dlaczego jest istotna i jak ją wdrożyć
- Identyfikowanie zagrożeń – jak wdrożyć odpowiednie rozwiązania na przestrzeganie zasad bezpieczeństwa
- Przegląd znanych typów ataków na JST - najnowsze zagrożenia
- Podstawy prawne i główne zasady cyberbezpieczeństwa
- Bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
 - ✓ Wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa
 - ✓ Wymagania dla pracowników wynikające z KRI, UoKSC oraz RODO
 - ✓ System Zarządzania Bezpieczeństwem Informacji w praktyce
- Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
 - ✓ Ochrona informacji i prywatność w internecie
 - ✓ Ransomware jako poważne zagrożenie dla JST
 - ✓ Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise)
 - ✓ Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne
 - ✓ Bezpieczne hasła i uwierzytelnienie dwuskładnikowe
 - ✓ Wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

Potwierdzeniem udziału kadry kierowniczej i pracowników w szkoleniu będzie imienna lista obecności.

Uwaga.

W przypadku gdy przywoływane przez Zamawiającego „aktualne normy” nie posiadają oficjalnej, polskiej wersji językowej osiągalnej za pośrednictwem Polskiego Komitetu Normalizacyjnego Zamawiający dopuszcza zastosowanie ich wersji poprzedniej (wycofanej) opublikowanej w polskiej wersji językowej.