

OPIS PRZEDMIOTU ZAMÓWIENIA

OPZ

Aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
oraz przeprowadzenie audytu bezpieczeństwa informacji

Zamawiający:	Gmina Krzanowice
Przedmiot zamówienia:	Audyt bezpieczeństwa informacji zgodny z wymogami audytu końcowego projektu grantowego „Cyberbezpieczny Samorząd” wraz z aktualizacją dokumentacji SZBI (Systemu Zarządzania Bezpieczeństwem Informacji)
Podstawa prawna:	KRI, RODO, UoKSC, NIS-2, ISO/IEC 27001

1. Postanowienia ogólne

1.1. Cel zamówienia

Przedmiotem zamówienia jest wykonanie kompleksowej usługi z zakresu bezpieczeństwa informacji dla **URZĘDU MIEJSKIEGO W KRZANOWICACH**

UL. MORAWSKA 5, 47-470 KRZANOWICE

obejmującego:

- przeprowadzenie audytu wstępnego bezpieczeństwa informacji dla jednostki,
- dokonanie przeglądu oraz aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- świadczenie konsultacji z zakresu bezpieczeństwa informacji i wdrożenia SZBI.

Zamówienie realizowane jest w celu zapewnienia zgodności z obowiązującymi przepisami prawa, w szczególności z:

- Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI),
- Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC),
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
- Dyrektywą NIS-2 i przepisami wdrażającymi,
- Normą PN-EN ISO/IEC 27001:2023-08.

1.2. Charakterystyka jednostki

Poniższa charakterystyka jednostki objętej zamówieniem stanowi podstawę przygotowania i wyceny oferty:

Parametr	Wartość
Nazwa jednostki	URZĄD MIEJSKI W KRZANOWICACH
Liczba pracowników (etatów)	43
Liczba lokalizacji (adresów) objętych zamówieniem	1
Liczba stacji roboczych	28
Liczba serwerów (fizycznych / wirtualnych)	3
Kluczowe systemy teleinformatyczne	EZD: MADKOM EZD SIDAS, INFO-SYSTEM GROSZEK (pakiet budżetowo-płacowo-podatkowy), Asseco Płatnik, Bestia;
Monitoring wizyjny	TAK
Prowadzenie naborów na stanowiska urzędnicze	TAK
Dopuszczenie urządzeń prywatnych do celów służbowych (BYOD)	NIE
Istniejąca dokumentacja SZBI	TAK – rok 2023

Informacje zawarte w charakterystyce jednostki rozstrzygają również o tym, które dokumenty oznaczone gwiazdką (*) w wykazie zawartym w Rozdziale 4 podlegają opracowaniu.

1.3. Definicje

Ilekoć w niniejszym OPZ jest mowa o:

- dniach roboczych – rozumie się przez to dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy,
- dniu stacjonarnym – rozumie się przez to dzień roboczy obejmujący co najmniej 8 godzin zegarowych obecności personelu Wykonawcy w siedzibie jednostki,
- jednostce – rozumie się przez to jednostkę objętą zamówieniem, wskazaną w pkt 1.2.

2. Zakres przedmiotowy zamówienia

2.1. Etap I – Audyt wstępny bezpieczeństwa informacji

2.1.1. Cel audytu

Celem audytu wstępnego jest kompleksowa ocena aktualnego stanu bezpieczeństwa informacji w jednostce objętej zamówieniem, umożliwiająca identyfikację luk i obszarów wymagających poprawy, stanowiąca podstawę dla dalszych prac wdrożeniowych lub aktualizacyjnych.

2.1.2. Zakres audytu

Audyt wstępny obejmuje następujące obszary:

- ocenę zgodności z Krajowymi Ramami Interoperacyjności (KRI), Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UoKSC) i innymi obowiązującymi wymaganiami prawnymi oraz normatywnymi,
- przegląd istniejącej dokumentacji SZBI i Polityk Bezpieczeństwa Informacji pod kątem kompletności, aktualności i zgodności z przepisami,
- analizę ryzyk w obszarze bezpieczeństwa informacji z uwzględnieniem specyfiki działalności danej jednostki,
- ocenę infrastruktury IT, w tym inwentaryzację systemów teleinformatycznych, serwerów, urządzeń sieciowych i stacji roboczych,
- ocenę wdrożonych zabezpieczeń fizycznych i środowiskowych w obszarach przetwarzania danych,
- kontrolę dostępu do systemów teleinformatycznych i pomieszczeń, w tym zarządzanie uprawnieniami,
- weryfikację przeprowadzonych szkoleń pracowników z zakresu bezpieczeństwa informacji i poziomu świadomości personelu,
- ocenę procedur wykrywania i reagowania na incydenty bezpieczeństwa informacji,
- analizę przygotowania planów ciągłości działania i odtwarzania po awarii,
- ocenę współpracy z podmiotami zewnętrznymi, w tym weryfikację umów, klauzul bezpieczeństwa i zapisów SLA.

2.1.3. Wymagania dotyczące obecności stacjonarnej – Etap I

Wykonawca jest zobowiązany do przeprowadzenia audytu wstępnego z zachowaniem minimum 4 (czterech) dni stacjonarnych, o następującym podziale:

Dzień audytu	Min. czas stacjonarny	Zakres działań
1 dzień - Spotkanie otwierające i przegląd dokumentacji	min. 8 godz.	Spotkanie z kierownictwem i IOD, zebranie dokumentacji, omówienie zakresu i metodyki audytu, wypełnienie ankiet wstępnych
2 dni - Audyt właściwy (wywiady, oględziny)	min. 16 godz. (2 dni)	Wywiady z kluczowym personelem, przegląd infrastruktury IT i pomieszczeń, weryfikacja systemu uprawnień, ocena zabezpieczeń fizycznych i kopii zapasowych
1 dzień - Spotkanie zamykające i omówienie wyników	min. 8 godz.	Prezentacja wstępnych wyników audytu, omówienie zidentyfikowanych niezgodności i obszarów ryzyka, ustalenie priorytetów działań naprawczych

Łączna minimalna liczba dni stacjonarnych dla Etapu I: 4 dni robocze.

2.1.4. Rezultat Etapu I

Rezultatem Etapu I jest Raport z audytu wstępnego, zawierający:

- ocenę stanu aktualnego bezpieczeństwa informacji z odniesieniem do KRI, UoKSC, RODO i ISO 27001,
- odniesienie wyników audytu do wymagań w zakresie bezpieczeństwa informacji określonych w § 20 rozporządzenia KRI,
- wykaz zidentyfikowanych niezgodności i luk bezpieczeństwa,
- ocenę ryzyk z podziałem na kategorie: krytyczne, wysokie, średnie, niskie,
- rekomendacje działań naprawczych z określeniem priorytetów,
- harmonogram proponowanych działań wdrożeniowych.

Raport dostarczany jest w wersji elektronicznej (PDF + edytowalny .docx) w terminie ustalonym w harmonogramie realizacji, o którym mowa w Rozdziale 3 niniejszego OPZ.

2.2. Etap II – Dokumentacja SZBI

Wykonawca jest zobowiązany do przeprowadzenia przeglądu istniejącej dokumentacji SZBI i jej aktualizacji do zgodności z KRI, RODO, UoKSC, NIS-2 oraz normą PN-EN ISO/IEC 27001:2023-08.

Zakres prac obejmuje:

- inwentaryzację posiadanej dokumentacji i ocenę jej kompletności względem wymaganego wykazu (3 dni stacjonarne),
- identyfikację dokumentów wymagających aktualizacji wynikającej ze zmian prawnych, organizacyjnych lub technologicznych, praca zdalna Wykonawcy
- identyfikację dokumentów brakujących i ich opracowanie, praca zdalna Wykonawcy
- aktualizację treści dokumentów istniejących z zachowaniem lub poprawą struktury, praca zdalna Wykonawcy
- ujednolicenie formy i struktury całości dokumentacji, praca zdalna Wykonawcy
- weryfikację spójności między dokumentami – polityki, procedury, rejestry, formularze, praca zdalna Wykonawcy
- szkolenie – wizyta stacjonarna, formalne przekazanie, szkolenie kluczowych pracowników (1 dzień stacjonarny).

Szkolenie kluczowych pracowników obejmuje co najmniej jedną sesję szkoleniową trwającą minimum 3 godziny zegarowe, przeprowadzoną w siedzibie jednostki dla pracowników wskazanych przez Zamawiającego (nie więcej niż 15 osób).

2.2.1. Rezultat Etapu II

Rezultatem Etapu II jest kompletna dokumentacja SZBI dla jednostki, dostosowana do jej indywidualnej specyfiki, obejmująca wszystkie dokumenty wymienione w Rozdziale 4 niniejszego OPZ. Dokumentacja przekazywana jest w wersji elektronicznej (.docx, .xlsx dla rejestrów i formularzy tabelarycznych) wraz z podpisanym przez obie strony wykazem przekazanych dokumentów.

2.3. Etap III – Konsultacje po wdrożeniu

W ramach Etapu III Wykonawca zobowiązuje się do świadczenia usług konsultacyjnych z zakresu bezpieczeństwa informacji i wdrożonego SZBI.

Parametr	Wartość / Opis
Łączny wymiar konsultacji	16 godzin
Forma	Zdalna (telefonicznie, e-mail, wideokonferencja) lub stacjonarna – do uzgodnienia między stronami
Czas reakcji	Do 2 dni roboczych od zgłoszenia przez Zamawiającego
Okres świadczenia	Od rozpoczęcia Etapu II do dnia zakończenia realizacji zamówienia, o którym mowa w Rozdziale 3
Ewidencjonowanie	Miesięczny rejestr wykorzystanych godzin konsultacyjnych przekazywany Zamawiającemu na żądanie

Konsultacje obejmują w szczególności:

- wsparcie w operacyjnym stosowaniu procedur i rejestrów SZBI,
- odpowiedzi na pytania pracowników i kierownictwa dotyczące wdrożonej dokumentacji,
- pomoc w reagowaniu na incydenty bezpieczeństwa informacji,
- wsparcie w kontaktach z organami nadzorczymi (UODO, właściwy CSIRT),
- bieżące informowanie o zmianach prawnych wpływających na wdrożone SZBI,
- wsparcie przy pierwszym przeglądzie zarządzania SZBI.

3. Termin i harmonogram realizacji

3.1. Termin realizacji zamówienia

Zamówienie zostanie zrealizowane w terminie 24 dni od dnia podpisania umowy.

Za dotrzymanie terminu realizacji zamówienia (oraz terminów poszczególnych Etapów) uważa się pisemne zgłoszenie przez Wykonawcę gotowości do odbioru prac wraz z przekazaniem Zamawiającemu kompletu rezultatów danego Etapu. Procedura odbioru, o której mowa w pkt 5.4, przeprowadzana jest po tym zgłoszeniu.

3.2. Harmonogram etapów

Poszczególne Etapy zamówienia realizowane są w następujących terminach:

Etap	Termin realizacji
Etap I – Audyt wstępny	Najpóźniej 18 dni do terminu końcowego umowy;
Etap II – Dokumentacja SZBI	Najpóźniej 10 dni do terminu końcowego umowy;
Etap III – Konsultacje	Najpóźniej 3 dni do terminu końcowego umowy;

W terminie 3 dni roboczych od dnia zawarcia umowy Strony uzgodnią szczegółowy harmonogram wizyt stacjonarnych, uwzględniający dostępność personelu jednostki.

4. Wykaz wymaganych dokumentów SZBI

Poniższy wykaz określa minimalny komplet dokumentów, który musi zostać opracowany lub zaktualizowany w ramach realizacji Etapu II. Wykonawca może zaproponować dodatkowe dokumenty uzasadnione specyfiką danej jednostki.

Lp.	Nazwa dokumentu	Typ
1.	Księga Bezpieczeństwa Informacji	Polityka/Deklaracja
2.	Polityka Bezpieczeństwa Informacji	Polityka/Deklaracja
3.	Cele bezpieczeństwa informacji	Polityka/Deklaracja
4.	Procedura postępowania z dokumentami	Procedura
5.	Procedura zarządzania dokumentacją systemów zarządzania	Procedura
6.	Słownik pojęć i skrótów	Dokument
7.	Wniosek o wprowadzenie zmian w dokumentacji SZBI	Formularz/Wzór
8.	Wykaz dokumentacji systemu zarządzania bezpieczeństwem informacji	Rejestr/Wykaz
9.	Polityka bezpieczeństwa przetwarzania danych osobowych	Polityka/Deklaracja
10.	Formularz realizacji żądań podmiotu danych	Formularz/Wzór
11.	Umowa powierzenia przetwarzania danych osobowych bez podpowierzenia – wzór	Formularz/Wzór
12.	Umowa powierzenia przetwarzania danych osobowych wraz z podpowierzeniem – wzór	Formularz/Wzór

13.	Rejestr umów powierzenia przetwarzania danych	Rejestr/Wykaz
14.	Upoważnienie do przetwarzania danych osobowych – wzór	Formularz/Wzór
15.	Oświadczenie o zachowaniu poufności	Formularz/Wzór
16.	Rejestr osób upoważnionych do przetwarzania danych osobowych	Rejestr/Wykaz
17.	Rejestr Czynności Przetwarzania Danych Osobowych (RCPD)	Rejestr/Wykaz
18.	Rejestr Kategorii Czynności Przetwarzania	Rejestr/Wykaz
19.	Wykaz budynków i pomieszczeń tworzących obszar przetwarzania danych osobowych	Rejestr/Wykaz
20.	Polityka naboru, zatrudnienia i rozwiązywania zatrudnienia	Polityka/Deklaracja
21.	Wniosek o przyjęcie nowego pracownika	Formularz/Wzór
22.	Opis stanowiska pracy	Formularz/Wzór
23.	Ogłoszenie o naborze na wolne stanowisko urzędnicze *	Formularz/Wzór
24.	Kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie	Formularz/Wzór
25.	Klauzula informacyjna dla osoby ubiegającej się o zatrudnienie	Formularz/Wzór
26.	Ocena warunków formalnych kandydatów na wolne stanowiska urzędnicze *	Formularz/Wzór
27.	Kryteria oceny kandydatów na wolne stanowiska urzędnicze *	Formularz/Wzór
28.	Protokół z przeprowadzonego naboru kandydatów na stanowisko pracy *	Formularz/Wzór
29.	Kwestionariusz osobowy dla pracownika	Formularz/Wzór
30.	Protokół zdawczo-odbiorczy	Formularz/Wzór
31.	Karta szkolenia wstępnego ochrony danych osobowych	Formularz/Wzór
32.	Klauzula informacyjna dla pracownika	Formularz/Wzór
33.	Polityka bezpieczeństwa fizycznego i środowiskowego	Polityka/Deklaracja
34.	Ewidencja wydania/przyjęcia klucza – wzór	Formularz/Wzór
35.	Rejestr kluczy – wzór	Rejestr/Wykaz
36.	Polityka bezpieczeństwa systemów teleinformatycznych	Polityka/Deklaracja
37.	Rejestr aktywów	Rejestr/Wykaz
38.	Rejestr kopii zapasowych	Rejestr/Wykaz
39.	Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych	Procedura
40.	Procedura użytkownika systemu teleinformatycznego	Procedura
41.	Polityka czystego biurka i czystego ekranu	Polityka/Deklaracja
42.	Polityka pracy zdalnej i korzystania z urządzeń mobilnych	Polityka/Deklaracja
43.	Wniosek o stałą/hybrydową pracę zdalną	Formularz/Wzór

44.	Wniosek pracownika o okazjonalną pracę zdalną	Formularz/Wzór
45.	Procedura korzystania z urządzeń prywatnych – BYOD *	Procedura
46.	Zgoda na wykorzystanie urządzeń prywatnych do celów służbowych *	Formularz/Wzór
47.	Umowa o użytkowanie sprzętu prywatnego do celów służbowych *	Formularz/Wzór
48.	Zgoda na wykorzystanie prywatnego numeru telefonu lub poczty e-mail *	Formularz/Wzór
49.	Procedura korzystania z narzędzi sztucznej inteligencji (AI)	Procedura
50.	Regulamin funkcjonowania monitoringu wizyjnego *	Dokument
51.	Wniosek o udostępnienie danych z monitoringu *	Formularz/Wzór
52.	Protokół przekazania na nośniku elektronicznym danych z systemu monitoringu *	Formularz/Wzór
53.	Rejestr nagrań z monitoringu wizyjnego *	Rejestr/Wykaz
54.	Ewidencja osób upoważnionych do wglądu do nagrań *	Rejestr/Wykaz
55.	Rysunek poglądowy lokalizacji kamer *	Dokument
56.	Informacja o przetwarzaniu danych w zakresie monitoringu wizyjnego *	Formularz/Wzór
57.	Polityka zarządzania ciągłością działania systemów teleinformatycznych	Polityka/Deklaracja
58.	Lista krytycznych systemów teleinformatycznych	Rejestr/Wykaz
59.	Plan ciągłości działania – wzór	Formularz/Wzór
60.	Raport z wykonania testu ciągłości działania	Formularz/Wzór
61.	Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi	Polityka/Deklaracja
62.	Formularz oceny podmiotu zewnętrznego	Formularz/Wzór
63.	Procedura przeprowadzania audytów	Procedura
64.	Roczny plan audytów – wzór	Formularz/Wzór
65.	Plan audytu – wzór	Formularz/Wzór
66.	Raport z audytu – wzór	Formularz/Wzór
67.	Raport z przeglądu zarządzania – wzór	Formularz/Wzór
68.	Rejestr niezgodności	Rejestr/Wykaz
69.	Procedura zarządzania incydentami	Procedura
70.	Katalog zagrożeń i incydentów bezpieczeństwa informacji	Dokument
71.	Formularz zgłoszenia zdarzenia	Formularz/Wzór
72.	Protokół zabezpieczenia materiału dowodowego	Formularz/Wzór
73.	Rejestr zdarzeń, naruszeń i incydentów	Rejestr/Wykaz
74.	Procedura zarządzania ryzykiem	Procedura
75.	Deklaracja stosowania (SoA)	Polityka/Deklaracja

76.	Tabela szacowania i postępowania z ryzykiem	Rejestr/Wykaz
77.	Raport z szacowania ryzyka	Dokument
78.	Plany postępowania z ryzykiem	Dokument
79.	Polityka klasyfikacji informacji	Polityka/Deklaracja
80.	Procedura zarządzania podatnościami technicznymi (Patch Management)	Procedura
81.	Procedura zarządzania zmianą w systemach teleinformatycznych	Procedura
82.	Procedura bezpiecznego niszczenia nośników danych	Procedura

* Dokumenty oznaczone gwiazdką opracowywane są wyłącznie wtedy, gdy dany obszar dotyczy specyfiki jednostki (prowadzenie naborów na stanowiska urzędnicze, dopuszczenie urządzeń prywatnych do celów służbowych, funkcjonowanie monitoringu wizyjnego) – zgodnie z charakterystyką jednostki określoną w pkt 1.2.

Dokumentacja musi być opracowana w plikach .docx (dokumenty tekstowe) oraz .xlsx (rejestry, formularze tabelaryczne, arkusze szacowania ryzyka, SoA). Format PDF dopuszczany wyłącznie jako wersja archiwalna, nie jako jedyna dostarczona forma.

5. Wymagania ogólne dotyczące realizacji zamówienia

5.1. Wymagania dotyczące personelu Wykonawcy

Wykonawca skieruje do realizacji zamówienia co najmniej 2 (dwie) osoby, z których każda posiada:

- co najmniej dwa z poniższych certyfikatów:
 - Certified Internal Auditor (CIA);
 - Certified Information Systems Auditor (CISA);
 - certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001, wydany przez jednostkę oceniającą zgodność akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
 - certyfikat audytora wiodącego systemu zarządzania ciągłością działania według normy PN-EN ISO 22301, wydany przez jednostkę oceniającą zgodność akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
 - Certified Information Security Manager (CISM);
 - Certified in Risk and Information Systems Control (CRISC);
 - Certified in the Governance of Enterprise IT (CGEIT);
 - Certified Information Systems Security Professional (CISSP);
 - Systems Security Certified Practitioner (SSCP);
 - Certified Reliability Professional;
 - Certyfikaty uprawniające do posługiwania się tytułem ISA/IEC 62443 Cybersecurity Expert.

Spełnienie powyższych wymagań Wykonawca wykaże w wykazie osób skierowanych do realizacji zamówienia, obejmującym informacje o doświadczeniu każdej z tych osób oraz o posiadanych certyfikatach. Zamawiający zastrzega sobie prawo żądania przedłożenia kopii certyfikatów oraz dokumentów potwierdzających doświadczenie przed zawarciem umowy.

5.2. Poufność i ochrona danych

Wykonawca zobowiązuje się do:

- zachowania poufności wszelkich informacji uzyskanych w trakcie realizacji zamówienia,
- nieprzekazywania dokumentacji i informacji uzyskanych od Zamawiającego podmiotom trzecim bez pisemnej zgody Zamawiającego,
- trwałego usunięcia lub zwrotu nośników zawierających dane jednostek po zakończeniu realizacji zamówienia.

5.3. Komunikacja i raportowanie

W trakcie realizacji zamówienia Wykonawca zobowiązuje się do:

- wyznaczenia dedykowanego opiekuna projektu dostępnego w godzinach roboczych,
- informowania Zamawiającego o postępie prac nie rzadziej niż raz na dwa tygodnie,
- niezwłocznego informowania Zamawiającego o zagrożeniach dla terminowości lub jakości realizacji zamówienia.

5.4. Odbiór prac

Każdy Etap zamówienia kończy się formalnym odbiorem prac potwierdzonym protokołem odbioru podpisanym przez Wykonawcę i upoważnionego przedstawiciela Zamawiającego. Zamawiający ma prawo do wniesienia uwag w terminie 5 dni roboczych od daty dostarczenia rezultatów danego Etapu; niewniesienie

uwag w tym terminie jest równoznaczne z odbiorem prac bez zastrzeżeń. Wykonawca jest zobowiązany do uwzględnienia uzasadnionych uwag w terminie 5 dni roboczych od ich otrzymania. Procedura odbioru obejmuje jedną rundę uwag i poprawek; po uwzględnieniu uzasadnionych uwag Zamawiający dokonuje odbioru prac. Zgłoszenie prac do odbioru w terminie, o którym mowa w Rozdziale 3, uważa się za dotrzymanie terminu realizacji.