|  |  |
| --- | --- |
| Numer sprawy: **OR.III.271.1.2025** | Kiwity dnia 26.06.2025 |
| Szczegółowy Opis Przedmiotu Zamówieniapn. Aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacjidla Gminy Kiwity |

Spis treści

[1. Przedmiot zamówienia 3](#_Toc176275598)

[1.1. Wymagania ogólne. 3](#_Toc176275599)

[1.2. Zakup usług aktualizacji i wdrożenia SZBI. 4](#_Toc176275600)

[2. Równoważność rozwiązań. 9](#_Toc176275601)

# Przedmiot zamówienia

# Wymagania ogólne.

1. Zamówienie będzie realizowane na rzecz Urzędu Gminy Kiwity.
2. Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Kiwity w ramach realizacji projektu pn. „Cyberbezpieczny Samorząd” współfinansowanego w ramach środków Unii Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II Zaawansowane usługi cyfrowe, Działania 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa.
3. Wykonawca jest odpowiedzialny za przeprowadzenie aktualizacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.
4. Aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:
	1. audytora zewnętrznego posiadającego 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) lub;
	2. audytora wewnętrznego posiadającego 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) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy **PN-EN ISO/IEC 27001:2023.**
5. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.
6. 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 zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
7. Na wszystkie usługi Wykonawca udzieli gwarancji do dnia 03.04.2026 r. polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.

# Zakup usług aktualizacji i wdrożenia SZBI.

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. 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, opracowania 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:
5. organizacja systemu bezpieczeństwa informacji;
6. zarządzanie aktywami;
7. zarządzanie zasobami ludzkimi;
8. organizacja bezpieczeństwa fizycznego i środowiskowego;
9. zarządzanie komunikacją i eksploatacją;
10. rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania;
11. kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
12. akwizycja, rozwój i utrzymanie systemu;
13. zarządzanie incydentami związanymi z bezpieczeństwem informacji;
14. zarządzanie ciągłością działania;
15. zarządzania kopiami zapasowymi;
16. zarządzania monitoringiem;
17. zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
18. używania urządzeń komputerowych;
19. metoda szacowania i postępowania z ryzykiem;
20. deklaracja stosowania
21. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć także aktualizację/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.

Ponad to:

1. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
2. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.
3. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
4. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI dla Zamawiającego.
5. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
6. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
7. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki.
8. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych.
9. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/systemy/usługi).
10. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
11. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
12. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem związanym z zagrożeniami bezpieczeństwa informacji.
13. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków.
14. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.
15. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
16. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
17. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
18. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami.
19. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
20. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.
21. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
22. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
23. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów.
24. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
25. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.

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-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:
8. Ocena schematu sieci.
9. Określenie rodzaju połączeń.
10. Określenie segmentów sieci.
11. Przeprowadzenie oceny środowiska informatycznego.
12. Ocena sposobu identyfikowania i logowania użytkowników.
13. Analiza zarządzania kontami użytkowników.
14. Analiza strony www i BIP pod kątem ochrony danych osobowych.
15. Analiza systemu backupów i archiwizacji danych.
16. Określenie miejsc redundancji w sieci i systemach informatycznych.
17. Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
18. Analiza konfiguracji zabezpieczeń baz danych.
19. Określenie bezpieczeństwa aplikacji i serwerów WWW.
20. Analiza konfiguracji urządzeń sieciowych: switche, routery, IDS, IPS, UTM, firewall.
21. Ocena zabezpieczeń dostępu do sieci publicznej.
22. Badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania.
23. Analiza zabezpieczeń stacji roboczych.
24. Analiza ochrony danych na komputerach przenośnych.
25. Badanie zabezpieczeń nośników zewnętrznych.
26. Sprawdzenie procedur zarządzania ciągłością działania.
27. 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:
3. określenie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
4. określenie zasięgu organizacji;
5. badanie środowiska zewnętrznego, powiązań z innymi organizacjami, systemami oraz dostawcami.
6. Zdefiniowanie wymaganych polityk SZBI:
7. uwzględnienie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
8. analiza wymagań prawnych oraz wymagań wynikających z umów;
9. uwzględnienie sposobu ustalania celów oraz wyznaczania kierunków działań w ramach systemu.
10. Szacowanie ryzyka:
11. wybór metody szacowania ryzyka;
12. określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
13. zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.
14. Wybór celów zabezpieczeń:
15. zdefiniowanie celów zabezpieczeń na podstawie listy zawartej w załączniku A normy **PN-EN ISO/IEC 27001:2023**;
16. zdefiniowanie własnych celów zabezpieczania i zabezpieczeń;
17. uwzględnienie wyników procesu szacowania ryzyka i określenie postępowania z ryzykiem;
18. 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:
4. przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
5. szacowanie i ocena ryzyka – zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
6. zdefiniowanie planu postępowania z ryzykiem;
7. określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
8. określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.
9. Opracowanie raportu z oceny ryzyka.

Etap V. Opracowanie niezbędnej dokumentacji SZBI.

1. Opracowanie wspólnie z pracownikami Zamawiającego wymaganych procedur i instrukcji:
2. opracowanie Polityki Bezpieczeństwa Informacji;
3. opracowanie Instrukcji Zarządzania Systemem Informatycznym;
4. opracowanie procedur i instrukcji wymaganych przez normę **PN-EN ISO/IEC 27001:2023**;
5. opracowanie procedur i instrukcji dopasowanych do specyfiki działalności organizacji;
6. opracowanie Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa;
7. opracowanie procedury audytu wewnętrznego;
8. opracowanie procedury nadzoru nad dokumentacją;
9. opracowanie procedury działań korygujących i zapobiegawczych;
10. opracowanie procedury zachowania ciągłości działania;
11. opracowanie wraz z pracownikami Zamawiającego planów ciągłości działania.
12. Wykonanie projektu zabezpieczeń - opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
13. Opracowanie programu uświadamiania i szkolenia.
14. Przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji.
15. 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:
4. przegląd zagrożeń;
5. przegląd podatności;
6. określenie i weryfikacja ryzyk;
7. weryfikacja planu postępowania z ryzykiem;
8. sprawdzenie zabezpieczeń i celów zabezpieczeń;
9. określenie zgodności zakresu SZBI;
10. weryfikacja zgodności z politykami i celami zabezpieczeń;
11. przegląd i ocena skuteczności zabezpieczeń;
12. weryfikacja zgodności wykorzystywania procedur;
13. weryfikacja zgodności obowiązków i uprawnień w ramach SZBI;
14. analiza audytów bezpieczeństwa;
15. weryfikacja dokumentacji i sposobu postępowania z incydentami;
16. weryfikacja sugestii oraz informacji zwrotnych od zainteresowanych stron;
17. sprawdzenie aktualności procedur ciągłości działania.
18. Opracowanie raportu z przeglądu.

# Równoważność rozwiązań.

1. Zamawiający informuje, że tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza się rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
2. Zamawiający informuje, że tam, gdzie w Zapytaniu oraz załącznikach opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne opisywanym pod warunkiem, że będą one o nie gorszych właściwościach i jakości. Zamawiający informuje, iż w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać materiały użyte do realizacji przedmiotu zamówienia. Ewentualne użycie nazwy producenta ma wyłącznie charakter przykładowy i ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania.
3. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez usługi spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.
4. Wykonawca, który posługuje się równoważnymi certyfikatami lub normami musi je załączyć do oferty. Przez certyfikat lub normę równoważną Zamawiający rozumie certyfikat lub normę analogiczną co do zakresu z certyfikatami lub normami wskazanymi z nazwy, który potwierdza spełnianie certyfikacji lub normy charakteryzującej się cechami właściwymi dla certyfikacji lub normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do certyfikacji.