IB.271.9.2026

Załącznik nr 1 Opis przedmiotu zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

I. NAZWA ZAMAWIAJĄCEGO

Gmina Serokomla, ul. Warszawska 21, 21-413 Serokomla

II. NAZWA ZADANIA

„Przeprowadzenie audytów i aktualizacja dokumentacji związanych z systemami bezpieczeństwa informacji w ramach realizacji projektu pn. „Cyberbezpieczny wodociąg Gmina Serokomla".

III. JEDNOSTKA OBJĘTA PRZEDMIOTEM ZAMÓWIENIA

Gminny Zakład Usług Komunalnych w Serokomli, ul. Warszawska 21, 21-413 Serokomla.

IV. TERMIN REALIZACJI ZAMÓWIENIA

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie od dnia zawarcia umowy do dnia 11 września 2026r.

V. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest:
   a) **Przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**

Ilość: 1 szt.

Opis	Aktualizacja istniejącej dokumentacji a w przypadku jej braku opracowanie i wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), obejmującego opracowanie polityk i procedur tematycznych, (adekwatnie do potrzeb organizacji), obejmujących wymaganiami normy ISO/IEC 27001:2023 następujące obszary: 1. Polityka bezpieczeństwa informacji. 2. Kontekst organizacji 3. Zarządzanie uprawnieniami dostępu do systemów i danych. 4. Zarządzanie personelem i bezpieczeństwo zasobów ludzkich. 5. Zarządzanie w obszarze świadomości personelu - szkolenia i świadomość bezpieczeństwa. 6. Zarządzanie aktywami. 7. Bezpieczeństwo fizyczne środowiskowe. 8. Bezpieczeństwo systemów informatycznych i sieci. 9. Praca zdalna. 10. Polityka ochrony przed szkodliwym oprogramowaniem. 11. Zarządzanie incydentami bezpieczeństwa. 12. Kopie zapasowe informacji. 13. Stosowanie kryptografii. 14. Monitorowanie i analiza zdarzeń związanych z bezpieczeństwem informacji. 15. Zarządzanie ryzykiem 16. Analiza ryzyka związanego z informacjami i danymi. 17. Określenie strategii i zarządzania ryzykiem. 18. Bezpieczeństwo relacji z dostawcami. 19. Ocena i wybór dostawców z uwzględnieniem bezpieczeństwa informacji. 20. Przechowywanie, znakowanie i udostępnianie dokumentacji. 21. Zarządzanie ciągłością działania. 22. Deklaracja stosowania zabezpieczeń

b) Audyt zgodności KRI

Ilość: 1 szt.

Opis	1. Polityka ciągłości działania; 2. określenie kontekstu organizacji; 3. określenie zakresu SZCD; 4. odpowiedzialność za planowanie ciągłości działania i zarządzanie kryzysowe; 5. przeprowadzenie analiza ryzyka i analizy wpływu na biznes (BIA); 6. opracowanie Planów ciągłości działania (BCP); 7. opracowanie procedur kryzysowych; 8. polityka informacyjna w przypadku wystąpienia sytuacji kryzysowej; 9. plany komunikacji, 10. przeprowadzenie audytów wewnętrznych w zaplanowanych odstępach czasu; 11. przeprowadzenie przeglądu zarządzania SZCD w zaplanowanych odstępach czasu;

c) Audyt cyberbezpieczeństwa sieci IT/OT/ICS/IIoT

Ilość: 1 szt.

Opis	Zakres audytu obejmuje zgodność z kryteriami zawartymi w § 19 ust. 2 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 307), lub zgodność z wymaganiami normy PN-ISO/IEC 27001. W szczególności zakres działań prowadzonych w ramach audytu ma obejmować weryfikację wymagań: 1. aktualizacja regulacji wewnętrznych; 2. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację; 3. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji 4. zapewnienie adekwatności poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji; 5. bezzwłoczna zmiana uprawnień, w przypadku zmiany zadań osób; 6. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji; 7. zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a. monitorowanie dostępu do informacji, b. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

	8. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość; 9. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie; 10. zawieranie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji; 11. ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych; 12. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a. dbałości o aktualizację oprogramowania, b. minimalizowaniu ryzyka utraty informacji w wyniku awarii, c. ochronie przed błędami, utratą, nieuprawnioną modyfikacją, d. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, e. zapewnieniu bezpieczeństwa plików systemowych, f. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, g. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, h. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa; 13. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób; 14. zapewnienie okresowego audytu w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

d) Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT

Ilość: 1 szt.

1. Analiza konfiguracji i bezpieczeństwa serwerów na poziomie systemu operacyjnego i usługowego
   a) sprawdzenie aktualności oprogramowania, obecności łatek systemowych,
   b) dostępność domyślnych kont użytkowników, bezpieczeństwo kont administratorskich, zgodność z polityką haseł,
   c) uruchomione usługi, ich celowość,
   d) zarządzanie systemami plików, polityka kopii zapasowych,
   e) zarządzanie ruchem sieciowym, zdalny dostęp, członkostwo w domenie,
   f) obecność i aktualność oprogramowania antywirusowego,
   g) logowane zdarzeń systemowych,
   h) zgodność konfiguracji z zewnętrznymi oraz wewnętrznymi standardami
2. Analiza konfiguracji i bezpieczeństwa na poziomie aktywnych urządzeń sieciowych
   a) aktualność oprogramowania, obecność łatek systemowych,
   b) dostępność domyślnych kont użytkowników, bezpieczeństwo kont, administratorskich, zgodność z polityką haseł,
   c) uruchomione usługi, ich celowość,
   d) logowane zdarzeń systemowych, podłączenie do systemów korelacji zdarzeń
3. Analiza konfiguracji i bezpieczeństwa na poziomie kanałów komunikacji pomiędzy poszczególnymi komponentami :
   a) weryfikacja ruchu sieciowego na poziomie aktywnych urządzeń sieciowych oraz usług udostępnionych na serwerach,
   b) weryfikacja użytych protokołów i ich konfiguracji,
   c) weryfikacja zabezpieczenia komunikacji pomiędzy poszczególnymi komponentami systemu informatycznego
4. Testy penetracyjne typu GreyBox obejmujące :
   a) aktywne urządzenia sieciowe (routery, drukarki, dyski i inne),
   b) potencjalne luki w systemach uwierzytelnienia,
   c) poziom bezpieczeństwa haseł,
   d) obecność kont typu “gość” oraz domyślnych haseł,
   e) identyfikację urządzeń dostępnych z poziomu internetu
   f) analizę topologii sieci z wewnątrz i z poziomu internetu,
   g) analizę bezpieczeństwa systemów operacyjnych i oprogramowania używanego przez pracowników,
   h) analizę bezpieczeństwa zapory sieciowej,

i) oszacowanie stopnia ryzyka wykrytych podatności

5. Przygotowanie raportu końcowego z przeprowadzonych testów bezpieczeństwa ze szczegółowym opisem wykrytych zagrożeń oraz rekomendacjami co do implementacji mechanizmów obronnych.

1. Wykonawca zobowiązany jest do opracowania dokumentacji powdrożeniowej wraz z ankietą dojrzałości oraz przygotowanie dokumentacji niezbędnej do rozliczenia projektu w ramach przedmiotowego zadania.
2. Zamówienie jest dofinansowane przez Unię Europejską w ramach programu Krajowy Plan Odbudowy i Zwiększenia Odporności, Priorytet C3: Cyberbezpieczeństwo. Działanie C3.1.1. Cyberbezpieczeństwo-CyberPL.
3. Kod CPV 79122000-3 Usługi audytu.
4. Zamawiający wymaga, aby Wykonawca posiadał lub dysponował dwiema osobami, z których każda posiada przynajmniej jeden z certyfikatów określonych 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 oraz posiadającą co najmniej dwuletnie doświadczenie zawodowe w zakresie przeprowadzania czynności audytowych. Wykaz certyfikatów wskazanych w ww. rozporządzeniu:
   1) Certified Internal Auditor (CIA);
   2) Certified Information System Auditor (CISA);
   3) 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 (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
   4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania 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;
   5) Certified Information Security Manager (CISM);
   6) Certified in Risk and Information Systems Control (CRISC);
   7) Certified in the Governance of Enterprise IT (CGEIT);
   8) Certified Information Systems Security Professional (CISSP);
   9) Systems Security Certified Practitioner (SSCP);
   10) Certified Reliability Professional;
   11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

VI. CZĘŚĆ INFORMACYJNA

1. Wykonawca powinien dokładnie i szczegółowo zapoznać się z Opisem przedmiotu zamówienia oraz wymaganiami określonymi w dokumentach projektu publikowanych na stronie https://www.gov.pl/web/cppc/cyberbezpieczne-wodociagi, zwracając uwagę na to, czy zawiera wszystkie informacje niezbędne do wykonania przedmiotu zamówienia.
2. Realizacja przedmiotu zamówienia terminowo.
3. Wykonawca jest zobowiązany do stałej współpracy z Zamawiającym na każdym etapie realizacji przedmiotu zamówienia, w celu koordynowania prawidłowego wykonania przedmiotu zamówienia, zgodnie z wytycznymi Zamawiającego.
4. Dokumentacja wchodząca w skład przedmiot umowy będzie sporządzona przez Wykonawcę i przekazana Zamawiającemu w formie cyfrowej oraz papierowej (2 egzemplarze).

Wójt Gminy Serokomla

/-/ Piotr Chaber