



OPIS PRZEDMIOTU ZAMÓWIENIA

Opracowanie, aktualizacja i wdrożenie SZBI, szkolenia oraz
przeprowadzenia audytu
w ramach projektu grantowego
pn. „Cyberbezpieczny Samorząd”

Priorytet II: Zaawansowane usługi cyfrowe

Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa
Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

80500000-9	Usługi szkoleniowe
72800000-8	Usługi audytu komputerowego i testowania komputerów



Cyberbezpieczny Samorząd

I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO

1. Wprowadzenie

Celem realizowanego projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty. Realizacja projektu „**Poprawa cyberbezpieczeństwa informacji w Gminie Chorkówka**”, będzie obejmowała:

1. Opracowanie, aktualizację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz wdrożenie SZBI.
2. Podniesienie poziomu wiedzy i kompetencji pracowników, w tym kadry zarządzającej.
3. Przeprowadzenie audytów SZBI oraz ankiety końcowej do konkursu grantowego „Cyberbezpieczny Samorząd”.

2. Zakres przedmiotu zamówienia

2.1. Opracowanie/aktualizacja oraz wdrożenie SZBI

Opracowanie/aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) składającego się m.in. z :

1. Polityki Bezpieczeństwa Informacji,
2. Deklaracji Stosowania,
3. Polityki Zarządzania Systemem Informatycznym,
4. Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania,
5. Polityki Zarządzania Incydentami Cyberbezpieczeństwa,
6. Polityki Ochrony Danych,
7. Analizy Zagrożeń i Ryzyka Bezpieczeństwa Informacji i Danych Osobowych.

Wewnętrzne polityki powinny uwzględniać m.in. następujące zagadnienia:

- określenie aktywów,
- klasyfikację informacji,
- procedury korzystania z urządzeń mobilnych,
- procedury pracy zdalnej, postępowanie z nośnikami,
- procedury kontroli dostępu,
- zasady nadawania uprawnień,
- zabezpieczenie pomieszczeń i obiektów,
- procedury czystego biurka,
- procedury czystego ekranu,
- procedury kopii zapasowych,
- procedury ochrony logów,
- bezpieczeństwo komunikacji,
- zarządzanie bezpieczeństwem sieci,
- obieg informacji,
- przesyłanie informacji,
- procedury zarządzania incydentami,
- prywatność i ochrona danych osobowych,
- szacowanie ryzyka w obszarze bezpieczeństwa informacji i danych osobowych,
- plan zarządzania podatnościami,

str. 2



Cyberbezpieczny Samorząd

- plan reagowania na incydenty,
- plan przywracania.

Usługa do realizacji w następujących jednostkach:

- Urząd Gminy w Chorkówce (aktualizacja z uwzględnieniem obowiązującej dokumentacji, SZBI powinno uwzględniać wdrożony SZBI i uzupełnić go o brakujące elementy),
- Gminy Ośrodek Pomocy Społecznej w Chorkówce (opracowanie SZBI, SZBI powinno uwzględniać wdrożone polityki z zakresu ochrony danych i uzupełnić je o brakujące elementy),
- Centrum Usług Oświatowych w Chorkówce (opracowanie SZBI, SZBI powinno uwzględniać wdrożone polityki z zakresu ochrony danych i uzupełnić je o brakujące elementy),
- Wodociągi Gminne Gminy Chorkówka w Chorkówce (opracowanie SZBI, SZBI powinno uwzględniać wdrożone polityki z zakresu ochrony danych i uzupełnić je o brakujące elementy).

Dokumentację SZBI należy przygotować w zgodności z obowiązującymi przepisami prawnymi, w szczególności z:

- ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 1557 z późn. zm.);
- rozporządzeniem 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. poz. 773), zwane dalej „KRI”;
- ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077), zwaną dalej „KSC”;
- Rozporządzeniem 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), zwanym dalej „RODO”;
- Narodowymi Standardami Cyberbezpieczeństwa, zwane dalej „NSC”.

Wdrożenie SZBI musi zostać wykonane w modelu stacjonarnym (minimum jeden jedzień), w siedzibie Urzędu Gminy w Chorkówce oraz Gminnym Ośrodku Pomocy Społecznej w Chorkówce, Centrum Usług Oświatowych w Chorkówce, Wodociągach Gminnych Gminy Chorkówka.

Wymogi wobec osób opracowujących/aktualizujących oraz wdrażających SZBI:

- minimum 4 letnie doświadczenie zawodowe w zakresie bezpieczeństwa informacji i ochrony danych,
- opracowania co najmniej 10 dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z KRI, KSC, RODO, normą ISO/IEC 27001,
- posiadanie co najmniej 4 lat certyfikatu audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001.

2.2. Podniesienie poziomu wiedzy i kompetencji pracowników, w tym kadry zarządzającej

Przygotowanie programu szkolenia oraz przeprowadzenie szkoleń budujących świadomość cyberzagrożeń, cyberbezpieczeństwa, sposobów ochrony danych osobowych i informacji, dla kadry pracowniczej i kadry kierowniczej, w tym administratorów.



Cyberbezpieczny Samorząd

Minimalne wymagania co do organizacji szkoleń dla kadry kierowniczej:

- szkolenia przeprowadzone w formie stacjonarnej;
- czas trwania szkolenia: 4 godziny zegarowe;
- ilość grup szkoleniowych: 1;
- szkolenie zakończone wystawieniem certyfikatów dla każdego Uczestnika.

Minimalne wymagania co do organizacji szkoleń dla kadry pracowniczej:

- szkolenia przeprowadzone w formie stacjonarnej;
- czas trwania szkolenia dla każdej grupy: 4 godziny zegarowe;
- ilość grup szkoleniowych: 5;
- szkolenie zakończone wystawieniem certyfikatów dla każdego Uczestnika.

Wśród ww. grup będą pracownicy z następujących podmiotów:

- Urząd Gminy w Chorkówce, Chorkówka 175, 38-458 Chorkówka
- Gminy Ośrodek Pomocy Społecznej w Chorkówce, Chorkówka 189, 38-458 Chorkówka
- Centrum Usług Oświatowych w Chorkówce, Chorkówka 143, 38-458 Chorkówka
- Wodociągi Gminne Gminy Chorkówka, Chorkówka 143, 38-458 Chorkówka

Minimalny zakres szkolenia:

1. Główne założenia i wymagania prawne RODO, KRI, KSC.
2. Incydent bezpieczeństwa informacji - zasady postępowania w przypadku jego wystąpienia.
3. Naruszenie ochrony danych osobowych i zasady postępowania w przypadku jego wystąpienia.
4. Podstawowe zasady bezpieczeństwa informacji i danych osobowych (bezpieczeństwo fizyczne):
 - a) Zasada czystego biurka;
 - b) Zasada czystego ekranu;
 - c) Zasada czystego wydruku;
 - d) Zasada czystego kosza;
 - e) Bezpieczeństwo poczty elektronicznej;
 - f) Używanie zewnętrznych nośników.
5. Bezpieczeństwo pracy zdalnej.
6. Polityka bezpiecznych haseł (menadżer haseł, generowanie i dobór haseł, postępowanie z hasłami).
7. Najczęściej wykorzystywane metody ataków (socjotechnika, ransomware, phishing, spoofing, sim swap, ataki przez strony www, telefon, spam). Omówienie ataków na przykładach.
8. Podstawowe metody obrony i weryfikacji prób ataków, dobre praktyki.
9. Przeprowadzenie testu oceniającego zdobytą wiedzę.

Wymogi wobec osób szkolących:

- minimum 4 letnie doświadczenie zawodowe w zakresie bezpieczeństwa informacji oraz ochrony danych osobowych,
- doświadczenie z przeprowadzonych szkoleń z zakresu bezpieczeństwa informacji, ochrony danych i cyberzagrożeń - minimum 10 szkoleń,
- posiadanie co najmniej 4 lat certyfikatu audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001.



Cyberbezpieczny Samorząd

2.3. Przeprowadzenie audytów SZBI oraz ankiety końcowej do konkursu grantowego „Cyberbezpieczny Samorząd”

Przeprowadzenie audytu po opracowaniu/aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w:

- Urząd Gminy w Chorkówce, Chorkówka 175, 38-458 Chorkówka
- Gminy Ośrodek Pomocy Społecznej w Chorkówce, Chorkówka 189, 38-458 Chorkówka
- Centrum Usług Oświatowych w Chorkówce, Chorkówka 143, 38-458 Chorkówka
- Wodociągi Gminne Gminy Chorkówka, Chorkówka 143, 38-458 Chorkówka

Audyt musi zostać przeprowadzony w zakresie spełniającym wymagania określone w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd”. Audyt Bezpieczeństwa Informacji musi być zgodny z przepisami 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 (t. j. Dz. U. 2024 r., poz. 773).

Przygotowanie i przedstawienie planów audytów może nastąpić w formie zdalnej, natomiast przeprowadzenie audytu w trybie stacjonarnym, z przeprowadzonego audytu należy przygotować wstępny raport, do którego dany podmiot może zgłosić uwagi, następnie należy przedstawić z audytu raport końcowy.

Po przeprowadzonym audycie należy uzupełnić ankietę końcową - Ankieta Dojrzałości Cyberbezpieczeństwa wg załącznika Nr 6 do regulaminu konkursu grantowego „Cyberbezpieczny Samorząd”.

Wymogi wobec osób przeprowadzających audyt:

- 4 letnie doświadczenie zawodowe w dziedzinie bezpieczeństwa informacji,
- doświadczenie potwierdzone wykonaniem co najmniej 10 audytów SZBI,
- Osoba przeprowadzająca audyt musi posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

3. Ogólne wymagania Zamawiającego

Niniejszy dokument ma na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na wykonanie usług szkolenia, opracowania i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz przeprowadzenie audytu, których podstawowym celem jest podniesienie poziomu bezpieczeństwa informacji oraz zwiększenie odporności JST, w ramach projektu „Cyberbezpieczny Samorząd”.

Dokument zawiera opis wymagań, które muszą być zrealizowane tak aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.

Opisane w dokumencie wymagania należy traktować jako podstawowe i minimalne.

W postępowaniu mogą wziąć udział wykonawcy, którzy:

Są zdolni do wykonania przedmiotu zamówienia i spełniają warunki w zakresie:

- a. posiadania kompetencji/uprawnień do prowadzenia działalności zawodowej, o ile wynika to z odrębnych przepisów – złożą w tym zakresie oświadczenie,

str. 5



Cyberbezpieczny Samorząd

- b. sytuacji finansowej umożliwiającej realizację przedmiotu zamówienia – złożą w tym zakresie oświadczenie,
- c. posiadania potencjału technicznego i osobowego niezbędnego do wykonania przedmiotu zamówienia – złożą w tym zakresie oświadczenie,
- d. posiadania wiedzy i doświadczenia w wykonywaniu przedmiotu zamówienia - złożą w tym zakresie oświadczenie.

Ponadto:

- a. Zleceniobiorca zobowiązuje się do opracowania i dostarczenia Zamawiającemu wytworzonej dokumentacji oraz wyników audytu wraz z zaleceniami w wersji papierowej.
- b. Zakończenie prac musi zostać potwierdzone protokołem odbioru, podpisanym przez Wykonawcę i Zamawiającego.
- c. Brak rozpoczęcia działań w terminie 30 dni kalendarzowych od terminu złożenia oficjalnego zamówienia, upoważnia Zamawiającego do odstąpienia od zamówienia.

II. **TERMIN WYKONANIA ZAMÓWIENIA**

- 1. Termin zakończenia realizacji zamówienia: **30.04.2026 r.**
- 2. Powyższy termin należy rozumieć jako datę bezusterkowego odbioru końcowego przedmiotu zamówienia przez Zamawiającego .
- 3. Zamawiający zastrzega możliwość zmiany terminu w przypadku wydłużenia realizacji przedmiotowego projektu ale nie dłużej niż do **30.05.2026 r.**
- 4. Harmonogram szczegółowy realizacji przedmiotu zamówienia zostanie ustalony przez strony w terminie do 7 dni roboczych od daty zawarcia umowy.

III. **WARUNKI**

1. **Pozostałe wymagania od Wykonawcy**

- 1) Poza wykonanymi usługami, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia.
- 2) Wykonawca powinien ponadto uwzględnić w cenie w ramach kosztów dodatkowych:
 - a) koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego,
 - b) koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane,
 - c) koszty opracowania dokumentacji powykonawczej
- 3) Wykonawca zobowiązany jest do:
 - a) dokonywania z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
 - b) Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.

str. 6



Cyberbezpieczny Samorząd

- c) Udzielania na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.

2. Odbiór końcowy

Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji. Odbiory będą odbywać się zgodnie z zapisami w Umowie na realizację zamówienia.

Przed przystąpieniem do odbioru końcowego Wykonawca przygotowuje następujące dokumenty:

- a. Raport końcowy z audytu bezpieczeństwa systemu informacji przeprowadzonego w danej jednostce organizacyjnej Wykonawca jest zobowiązany sporządzić w wersji papierowej w ilości – 2 egz., oraz w wersji elektronicznej na zabezpieczonym nośniku informatycznym lub przekazany na wskazaną do kontaktu skrzynkę e-mail, w sposób zapewniający poufność przekazywanych danych.
- b. Przygotowana dokumentacja SZBI dla wskazanych w opisie zamówienia podmiotów, w wersji papierowej oraz elektronicznej na zabezpieczonym nośniku informatycznym lub przekazana na wskazaną do kontaktu skrzynkę e-mail, w sposób zapewniający poufność przekazywanych danych.
- c. Potwierdzeniem wykonania szkoleń będzie przekazanie Zamawiającemu list obowocności na szkoleniach, wyników testów (bez danych osobowych uczestników szkoleń) potwierdzających wzrost wiedzy i kompetencji z cyberbezpieczeństwa. Przekazanie certyfikatów szkolenia.
- d. Potwierdzeniem wykonania całości zamówienia będzie podpisany elektronicznie lub tradycyjnie protokół odbioru końcowego.

3. Dokumenty uzupełniające opis przedmiotu zamówienia: Regulamin konkursu grantowego „Cyberbezpieczny Samorząd”.