Załącznik nr 3 do SWZ

**Przeprowadzenie audytów w zakresie cyberbezpieczeństwa, opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji SZBI w Gminie Mieszkowice w ramach projektu „Cyberbezpieczna Gmina Mieszkowice”**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

l. Zamawiający:

Zamawiający prowadzi postępowanie o udzielenie zamówienia publicznego na realizację pn. Przeprowadzenie audytów w zakresie cyberbezpieczeństwa, opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji SZBI w Gminie Mieszkowice w ramach projektu „Cyberbezpieczna Gmina Mieszkowice”

w konkursie grantowym „Cyberbezpieczny Samorząd” realizowanym w ramach Priorytetu Il „Zaawansowane usługi cyfrowe”. Projekt współfinansowany jest ze środków Unii Europejskiej w ramach działania 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Przedmiot zamówienia realizowany będzie w:

1. Urzędzie Gminy Mieszkowice
2. Ośrodku Pomocy Społecznej w Mieszkowicach
3. Zespole Obsługi Szkół w Mieszkowicach

II. Przedmiot zamówienia

Zamówienie obejmuje 3 zadania:

1. **Zadanie 1: Przeprowadzenie audytu przedwdrożeniowego** **SZBI, oraz zgodności z KRI i uoKSC.**

Przeprowadzić audyt u Zamawiającego obejmujący audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i Polityki Bezpieczeństwa informacji, w tym zgodność z S 19 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. poz. 773) i wymogami ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077)

Zadanie nr 1 obejmie w szczególności przeprowadzenie analizy obecnie wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji. Wyniki analizy będą podstawą do dalszych prac.

Termin wykonania zadania: **do 31.10.2024**

1. **Zadanie nr 2: Opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji SZBI i PBI**

Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o wykonane analizy, Polską Normę PN-ISO/IEC 27001, ustawę z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, 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 MS 2), rozporządzenie 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), ustawę z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne oraz przepisów wykonawczych, zwierający niezbędne polityki i procedury, w szczególności:

* + zasady nadawania uprawnień,
	+ zasady tworzenia i zmiany haseł,
	+ zasady korzystania z systemów informatycznych,
	+ zasady pracy na odległość (przedstawić propozycje działań organizacyjnych i technicznych w celu bezpiecznego przetwarzania danych na komputerach i innych urządzeniach),
	+ okresowa kontrola dostępności,
	+ eksploatacja systemów i sieci, zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej,
	+ ochrona systemowa poczty przychodzącej,
	+ archiwizacja poczty,
	+ zasady wykonywania przeglądów zarządzania,
	+ zarządzanie wymiennymi nośnikami, - kopie bezpieczeństwa, - polityka postepowania z informacją, - klasyfikacja informacji,
	+ polityka czystego biurka i ekranu, - zarządzanie i nadzór nad incydentami, - pomiar skuteczności zabezpieczeń,
	+ plan ciągłości działania,
	+ plan postępowania z ryzykiem,
	+ zasady testowania skuteczności zabezpieczeń,
	+ skróconą dokumentację zawierającą podstawy dotyczące wybranych tematów SZBI niebędących informacją poufną dla pracowników.

- innych dokumentów, niezbędnych do zarządzania bezpieczeństwem informacji.

**Termin wykonania zadania: do 20.12.2024**

1. **Zadanie nr 3: Przeprowadzenie audytu powdrożeniowego SZBI, oraz zgodności z KRI i uoKSC**

Przeprowadzenie audytu wdrożonego u Zamawiającego Systemu Zarządzania Bezpieczeństwem Informacji, w zakresie obejmującym zgodność z kryteriami zawartymi w S 19 ust. 2 rozporządzenia, o którym mowa w pkt 1, lub zgodność z wymaganiami normy PNISO/IEC 27001 , czego wynikiem będzie sporządzenie raportu z audytu, zgodnie z wymogami Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02 -CS.01-001/23, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet Il: Zaawansowane usługi cyfrowe Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy.

Opracowany i wdrożony system SZBI powinien odnosić się do zapisów w kolumnie „Stan planowany” dla każdego działania z Załącznika Nr 6 do Umowy o powierzenie grantu pt. Ankieta Dojrzałości Cyberbezpieczeństwa – **załącznik nr 8 do SWZ.** Ankietę dojrzałości należy uzupełnić po przeprowadzeniu audytu.

**Termin wykonania zadania: do 20.12.2024**

**III. Obowiązki wykonawcy**

Zagadnienia dotyczące zabezpieczeń, zarządzania ryzykiem oraz audytowania powinny spełniać wymagania Polskich Norm PN-ISO/IEC 27002 (w odniesieniu do ustanawiania zabezpieczeń), PN-ISO/IEC 27005 (w odniesieniu do zarządzania ryzykiem) oraz PN-ISO/IEC 24762 (w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania).

Wykonawca zobowiązany jest do dostosowania SZBI do zmian przepisów lub Normy, o których mowa wyżej, jeżeli zmiana ta zostanie opublikowana w trakcie realizacji umowy.

Wykonawca zobowiązuje się do przedłożenia na etapie składania oferty następujących dokumentów potwierdzających spełnianie przez niego warunków udziału w postępowaniu:

1) w przypadku, gdy wykonawca jest audytorem zewnętrznym - 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. poz. 1999), tj.:

* 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.

 W przypadku, gdy wykonawca jest audytorem wewnętrznym - przynajmniej jeden z certyfikatów określonych w rozporządzeniu, o którym mowa w pkt 1, lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001 ;