Załącznik nr 5
do zapytania ofertowego
IN.041.1.2025 z dnia 4 marca 2025 r.

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ) – wykonanie audytu Systemu Zarządzania Bezpieczeństwem Informacji dla 8 jednostek organizacyjnych Gminy Jerzmanowa, opracowanie, wdrożenie, przegląd, aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Jerzmanowa oraz przeprowadzenie szkoleń z zakresu SZBI dla 8 jednostek organizacyjnych w ramach projektu pn. „Cyberbezpieczna Gmina Jerzmanowa".

1. Przedmiotem zamówienia jest wykonanie usługi polegającej na przeprowadzeniu audytu Systemu Zarządzania Bezpieczeństwem Informacji dla 8 jednostek organizacyjnych Gminy Jerzmanowa, opracowanie, wdrożenie, przegląd, aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Gminy Jerzmanowa oraz przeprowadzenie szkoleń z zakresu funkcjonowania i stosowania Systemu Zarządzania Bezpieczeństwem Informacji dla 8 jednostek organizacyjnych w ramach projektu pn. „Cyberbezpieczna Gmina Jerzmanowa".
2. Jednostki organizacyjne objęte przedmiotem zamówienia:
    1) Urząd Gminy Jerzmanowa, Jerzmanowa, ul. Lipowa 4, 67-222 Jerzmanowa,
    2) Szkoła Podstawowa im. Jana Pawła II w Jerzmanowej, Jerzmanowa, ul. Głogowska 19, 67 222 Jerzmanowa,
    3) Szkoła Podstawowa im. Henryka Sienkiewicza w Jaczowie, Jaczów, ul. Główna 20, 67-210 Jaczów,
    4) Przedszkole Gminne „Kraina Marzeń" w Jerzmanowej, Jerzmanowa, ul. Obiszowska 25, 67-222 Jerzmanowa,
    5) Przedszkole Gminne „Ocean Marzeń" w Jaczowie, Jaczów, ul. Smardzowska 1, 67-210 Jaczów,
    6) Żłobek Gminny w Jaczowie, Jaczów, ul. Główna 21L, 67-210 Jaczów,
    7) Gminny Ośrodek Pomocy Społecznej w Jerzmanowej, Jerzmanowa, ul. Głogowska 7, 67-222 Jerzmanowa,
    8) Zakład Gospodarki Komunalnej w Jerzmanowej, Jerzmanowa, ul. Głogowska 5, 67-222 Jerzmanowa.
3. Zadanie objęte jest dofinansowaniem w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd".
4. Zakres realizacji usługi obejmuje opracowanie, wdrożenie, przegląd, aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PNISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301 dla Urzędu Gminy Jerzmanowa. Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do

faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:

1) rozporządzenia 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),
2) ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.), 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. 2024 poz. 773).

5. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy **PN-EN ISO/IEC 27001:2023 lub równoważnej** dla Zamawiającego. *Za równoważne do normy PN-EN ISO/IEC 27001:2023 Zamawiający uzna inne normy dotyczące międzynarodowego standardu w zakresie bezpieczeństwa informacji obejmujące wymagania normy PN-EN ISO/IEC 27001:2023 określone w rozdziałach 4-10 tej normy.*
6. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.

I. **Wymagania stawiane wykonawcy:**

1. Wykonawca musi dysponować i przeznaczyć do realizacji zamówienia co najmniej jedną osobę będącą audytorem posiadającym 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) oraz posiadającą doświadczenie zawodowe w zakresie audytowania systemów zarządzania bezpieczeństwem informacji (SZBI).
2. Zamawiający wymaga aby wdrożenie SZBI w Urzędzie Gminy Jerzmanowa polegało na analizie oraz aktualizacji i wdrożeniu istniejącej u Zamawiającego Polityki Bezpieczeństwa Informacji (PBI) w sposób gwarantujący spełnienie wymagań norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301.
3. Na bazie istniejącej w Urzędzie Gminy Jerzmanowa Polityki Bezpieczeństwa Informacji Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:

1) rozporządzenia 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),
2) ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.), 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. 2024 poz. 773).

4. Kompletną dokumentację SZBI wraz z formularzami, opracowaniami zasad postepowania, procedur należy sporządzić w 2 egz. w wersji papierowej oraz 1 egz. w wersji elektronicznej na płycie CD/DVD.

II. Sposób realizacji zadania:

1. Zamawiający wymaga aby wszystkie prace związane z przeprowadzaniem wywiadów, ankiet i analiz wśród pracowników Zamawiającego realizowane były przez przedstawiciela Wykonawcy w siedzibach jednostek objętych audytem, określonych w pkt. 2 Opisu Przedmiotu Zamówienia;
2. Zamawiający wyklucza możliwość stosowania ankiet do samodzielnego wypełnienia przez pracowników Zamawiającego.
3. Zamawiający dopuszcza realizowanie czynności określonych w pkt. 1 w formie zdalnej, po uprzednim uzyskaniu zgody Zamawiającego.

III. Wymagania dotyczące Polityki Bezpieczeństwa Informacji:

1. Zamawiający wymaga aby wdrożona Polityka Bezpieczeństwa Informacji w sposób usystematyzowany oraz jednoznaczny opisywała i regulowała zagadnienia oraz obszary funkcjonowania wynikające bezpośrednio z celów stosowania zabezpieczeń stanowiących załącznik A do normy ISO/IEC 27001 oraz dyrektywy NIS-2.
2. Dokumentacja opisująca zasady funkcjonowania i kontroli systemu informatycznego powinna zawierać szablony wszystkich wykazów i rejestrów które powinny być prowadzone przez użytkowników lub administratorów systemu informatycznego.

IV. Wymagania dotyczące zakresu szkoleń dla kadry kierowniczej i pracowników:

1. Szkolenia z zakresu funkcjonowania i stosowania Systemu Zarządzania Bezpieczeństwem Informacji przeprowadzane będą w siedzibach jednostek organizacyjnych określonych w pkt. 2 Opisu Przedmiotu Zamówienia i powinny obejmować m.in.:
   1) wymogi wynikające z Krajowych Ram Interoperacyjności (KRI), Ustawa o krajowym systemie cyberbezpieczeństwa (UoKSC) i Ogólne rozporządzenie o ochronie danych (RODO),
   2) zarządzanie ryzykiem w bezpieczeństwie informacji,
   3) System Zarzadzania Bezpieczeństwem informacji – jak skutecznie przestrzegać procedur wdrożonej Polityki Bezpieczeństwa Informacji,
   4) ciągłość działania – dlaczego jest istotna i jak ją wdrożyć,

5) identyfikowanie zagrożeń – jak wdrożyć odpowiednie rozwiązania na przestrzeganie zasad bezpieczeństwa,
6) przegląd znanych typów ataków na JST - najnowsze zagrożenia,
7) podstawy prawne i główne zasady cyberbezpieczeństwa,
8) bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
    a. wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa,
    b. wymagania dla pracowników wynikające z KRI, UoKSC oraz RODO,
    c. System Zarządzania Bezpieczeństwem Informacji w praktyce,
9) Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
    a. ochrona informacji i prywatność w internecie,
    b. ransomware jako poważne zagrożenie dla JST,
    c. phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise),
    d. cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne,
    e. bezpieczne hasła i uwierzytelnienie dwuskładnikowe,
    f. wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

2. Potwierdzeniem udziału kadry kierowniczej i pracowników w szkoleniu będzie imienna lista obecności.