OPIS PRZEDMIOTU ZAMÓWIENIA

Kody i nazwy opisujące przedmiot zamówienia (CPV):

72 – 80 – 00 – 00 – 8 – usługi audytu komputerowego i testowania komputerów
72 – 81 – 00 – 00 – 1 – usługi audytu komputerowego\
79 – 21 – 20 – 00 – 3 – usługi audytu
79 – 13 – 10 – 00 – 1 – usługi w zakresie dokumentów
80 – 00 – 00 – 00 – 4 – usługi edukacyjne i szkoleniowe
80 – 50 – 00 – 00 – 9 – usługi szkoleniowe
80 – 55 – 00 – 00 – 4 – usługi szkolenia w dziedzinie bezpieczeństwa
80 – 53 – 20 – 00 – 2 – usługi szkolenia w dziedzinie zarządzania
80 – 51 – 00 – 00 – 2 – usługi szkolenia specjalistycznego
79 – 41 – 70 – 00 – 0 – usługi doradcze w zakresie bezpieczeństwa

Przedmiot zamówienia obejmuje wykonanie następujących zadań:

1) **Zadanie I:** Przeprowadzenie audytu wstępnego (przedwdrożeniowego) oraz końcowego (powdrożeniowego).
2) **Zadanie II:** Opracowanie dokumentacji i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
3) **Zadanie III:** Przeprowadzenie analizy ryzyka oraz oceny skutków przetwarzania danych osobowych (DPIA).
4) **Zadanie IV:** Przeprowadzenie szkoleń dla pracowników i kadry kierowniczej oraz szkoleń specjalistycznych dla pracowników IT.
5) **Zadanie V:** Wykonanie testów bezpieczeństwa i podatności.

1. Wykonawca oświadcza, że posiada wszelką niezbędną wiedzę, umiejętności i certyfikaty do wykonania przedmiotu zamówienia zgodnie z projektem grantowym pn. „Cyberbezpieczny Samorząd” dofinansowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Działania 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd”.
2. Wykonawca oświadcza, że dysponuje personelem posiadającym uprawnienia potwierdzone certyfikatami niezbędnymi do realizacji przedmiotu umowy, wydanymi zgodne z Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. 2018 r. poz. 1999) oraz zgodnie z projektem grantowym pn. „Cyberbezpieczny Samorząd” dofinansowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Działania 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd”, w tym również minimum 2 letnie doświadczenie w przedmiotowym zakresie.
3. Wszystkie dokumenty i materiały opracowane przez Wykonawcę winny zostać oznakowane za pomocą:
   1) znaku Fundusze Europejskie wraz z nazwą Programu,

2) barw Rzeczpospolitej Polskiej,
3) znaku Unii Europejskiej wraz ze słownym odniesieniem „Dofinansowane przez Unię Europejską”,
4) znaku Cyberbezpieczny Samorząd (po linii rozdzielającej).

4. Szczegółowe informacje i przykłady dotyczące zastosowania powyższych wymagań zostały określone w „Podręczniku wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji” oraz w Księdze Tożsamości Wizualnej marki Fundusze Europejskie 2021-2027. Materiały w formie elektronicznej są dostępne w serwisie internetowym pod adresem: www.funduszeeuropejskie.gov.pl.
5. W przypadku uwag do realizacji poszczególnych zadań Wykonawca musi dokonać stosownych korekt w terminie 5 dni roboczych od ich zgłoszenia.
6. Podstawą do wystawienia faktury i wypłaty wynagrodzenia będzie podpisany bez uwag i zastrzeżeń protokół odbioru końcowego.

Zadanie I: Przeprowadzenie audytu wstępnego (przedwdrożeniowego) oraz końcowego (powdrożeniowego)

1. Wymaga się przeprowadzenia dwóch audytów: wstępnego (przedwdrożeniowego) i końcowego (powdrożeniowego).
2. Audyty powinny uwzględniać specyfikę Urzędu oraz jego strukturę organizacyjną i lokalizację.
3. Audyty muszą być przeprowadzone przez osobę lub osoby posiadające stosowną wiedzę i minimum 2 letnie udokumentowane doświadczenie w przedmiotowym zakresie oraz co najmniej jeden certyfikat świadczący o posiadanej wiedzy w danym zakresie.
4. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z wypełnioną przez Zamawiającego ankietą dojrzałości cyberbezpieczeństwa oraz uwzględnić w ramach wdrożenia SZBI planowany zakres usprawnień.
5. W ramach audytu wstępnego Wykonawca przeprowadzi wizję lokalną w każdym z budynków Zamawiającego oraz dokona wywiadów z pracownikami.
6. Zamawiający nie dopuszcza wykonania audytu wstępnego w sposób zdalny.
7. Zakres audytu wstępnego (przedwdrożeniowego):
   1) Ocena poziomu bezpieczeństwa organizacyjnego związanego z aktualnie posiadaną dokumentacją i procedurami, w tym m.in.:
      a) weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
      b) odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
      c) dokumentacja, w tym z zakresu ochrony danych osobowych;
      d) analiza ryzyka;
      e) inwentaryzacja aktywów;
      f) inwentaryzacja wszystkich procesów przetwarzania danych osobowych;
      g) plan postępowania z ryzykiem;
      h) przeprowadzenie wywiadów z pracownikami Zamawiającego.
   2) Ocena poziomu bezpieczeństwa technicznego związanego z aktualnie posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością, w tym m.in.:
      a) weryfikacja zabezpieczeń wejścia/wyjścia;
      b) weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;

c) weryfikacja bezpieczeństwa okablowania strukturalnego;
a) weryfikacja systemów chłodzenia i systemów alarmowych;
b) weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi;
c) przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania i ciągłości działania;
d) weryfikacja ochrony przed oprogramowaniem szkodliwym;
e) weryfikacja procedur zarządzania kopiami zapasowymi;
f) weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
g) weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
h) weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);

3) Audyt wstępny (przedwdrożeniowy) musi obejmować w szczególności analizę czy wymagania określone w rozporządzeniu 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 zostały spełnione.

8. Efektem realizacji audytu wstępnego będzie zbiorczy raport przygotowany i przekazany Zamawiającemu w formie papierowej i elektronicznej. Raport będzie zawierał co najmniej:
   1) informację o stanie aktualnym i stwierdzonych uchybieniach,
   2) opis wykonania planu audytu,
   3) opis wykorzystanych standardów,
   4) ocenę spełnienia wymagań,
   5) wydanie rekomendacji (zaleceń pokontrolnych) w przypadku stwierdzonych niezgodności i braków, które będą stanowiły podstawę przygotowania i wdrożenia dokumentacji SZBI.
9. Termin i forma omówienia raportów: Spotkanie w siedzibie Urzędu, podczas którego wyniki audytu zostaną omówione z kadrą kierowniczą, w terminie do 14 dni licząc od dnia zakończenia czynności audytowych.
10. Wykonawca w sporządzonym raporcie, o którym mowa w ust. 9 opracuje założenia do Systemu Zarządzania Bezpieczeństwem Informacji, obejmujące listę wszystkich wymagań norm ze wskazaniem:
    1) proponowanych środków do realizacji wymagań z uwzględnieniem istniejących środków organizacyjnych i technicznych Zamawiającego
    2) działań niezbędnych do spełnienia poszczególnych wymagań na poziomie organizacyjnym i technicznym;
    3) statusu działań: zrealizowane/częściowo zrealizowane/niezrealizowane.
11. Zamawiający zastrzega sobie prawo do wniesienia uwag do zawartości raportu z przeprowadzonego audytu.

Audyt końcowy (powdrożeniowy):

1. Polegać będzie na ponownym dokonaniu analizy części formalnoprawnej oraz technologicznej, zgodnie z założeniami audytu wstępnego oraz skuteczności realizacji **zadania II,** tj. opracowanie dokumentacji i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

2. W ramach audytu końcowego Zamawiający wymaga wykonania końcowej ankiety dojrzałości stanu cyberbezpieczeństwa zgodnie z wytycznymi Konkursu Grantowego Cyberbezpieczny Samorząd Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
3. Efektem realizacji audytu końcowego (powdrożeniowego) będzie zbiorczy raport przygotowany i przekazany Zamawiającemu w formie papierowej i elektronicznej. Raport będzie zawierał co najmniej:
   1) informację o stanie przygotowania organizacyjno-technicznego Urzędu po wdrożeniu SZBI,
   2) opis wykonania planu audytu,
   3) opis wykorzystanych standardów,
   4) ocenę spełnienia wymagań,
   5) wydanie rekomendacji (zaleceń pokontrolnych) w przypadku stwierdzonych niezgodności i braków, które nie zostały zrealizowane podczas wdrożenia SZBI.

Zadanie II: Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1. W ramach usługi Wykonawca dokona opracowania dokumentacji i przeprowadzi kompleksowe wdrożenie Systemu Zarządzania Bezpieczeństwa Informacji w Urzędzie Miasta Ciechanów.
2. Poprzez wdrożenie należy rozumieć m.in.:
   1) przegląd obecnie posiadanej dokumentacji, w tym m.in.:
      a) Polityki Ochrony Danych Osobowych w Urzędzie Miasta Ciechanów;
      b) Instrukcji zarządzania zasobami informatycznymi Urzędu Miasta Ciechanów;
      c) Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w Urzędzie Miasta Ciechanów;
      d) Metodyka szacowania ryzyka dla danych osobowych przetwarzanych w Urzędzie Miasta Ciechanów;
      e) Polityki ochrony danych osobowych przetwarzanych w Systemie Miejskiego Monitoringu Wizyjnego;
      f) Polityki Bezpieczeństwa Informacji w Straży Miejskiej;
      g) Analizie ryzyka ogólnego i oceny skutków dla przetwarzania danych (DPIA) w Straży Miejskiej;
      h) Regulaminu funkcjonowania Systemu Monitoringu Wizyjnego – Kamery personalne w Straży Miejskiej;
      i) inne regulaminy i procedury Zamawiającego.
   2) dokonanie ewentualnej implementacji, koordynacji, aktualizacji z SZBI,
   3) opracowanie dokumentacji SZBI zgodnie z wymogami 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,
   4) utworzenie odpowiednich dokumentów/procedur/instrukcji, nowe metodologie zarządzania ryzykiem u Zamawiającego - w postaci gotowych zapisów/regulacji/procedur, do zatwierdzenia przez Kierownictwo Zamawiającego,

5) zinwentaryzowanie wszystkich procesów przetwarzania danych osobowych. W efekcie wymaga się opracowania Rejestru Czynności Przetwarzania (RCP) oraz Rejestru Kategorii Czynności Przetwarzania (RKCP) dedykowanego na każdy z wydziałów, referatów, samodzielnych stanowisk oraz jeden połączony w całość z wyszczególnionymi procesami "wspólnymi" dla wszystkich referatów, wydziałów, samodzielnych stanowisk.
6) przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

3. Zakres działań na rzecz realizacji zadania:
   1) Ocena bieżących praktyk w obszarze bezpieczeństwa informacji oraz analiza istniejącej dokumentacji z obszaru bezpieczeństwa informacji i ochrony danych osobowych, stosowanych zabezpieczeń technicznych i organizacyjnych.
   2) Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w oparciu o wyniki przeprowadzonego wcześniej audytu wstępnego, dokonanie aktualizacji lub doskonalenie istniejącej dokumentacji, a w przypadku braku opracowanie polityki bezpieczeństwa informacji zgodnej z wymaganiami najnowszych wersji serii norm ISO, a w szczególności PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO 22301 oraz PN-EN ISO 22313;
   3) Opracowanie Deklaracji stosowania zabezpieczeń wg. wymagań Załącznika A normy PN-EN ISO/IEC 27001:2023.
   4) Zapoznanie pracowników Zamawiającego w zakresie zadań i wymogów wynikających z wdrażanej dokumentacji SZBI, np. podczas szkoleń realizowanych w ramach **Zadania IV,** tj. przeprowadzenie szkoleń dla pracowników oraz kadry kierowniczej.
4. Wykonawca zobowiązany jest wytworzyć dokumentację SZBI spójną, jednolitą oraz adekwatną do rzeczywistych ryzyk, procesów i potrzeb Zamawiającego, uwzględniając przy tym specyfikę i strukturę organizacyjną oraz wszystkich lokalizacji Zamawiającego.
5. Wykonawca opracowując SZBI uwzględni zmieniającą się infrastrukturę teleinformatyczną Zamawiającego.
6. Zamawiający planuje, w okresie świadczenia usługi przez Wykonawcę, rozbudowę infrastruktury teleinformatycznej.
7. Wykonawca przygotuje harmonogram dostosowywania opracowywania poszczególnych elementów SZBI.
8. Harmonogram realizacji zadań musi uwzględniać przekazywanie przez Wykonawcę poszczególnych dokumentów etapami, w sposób pozwalający na weryfikację dokumentów przez Zamawiającego.
9. Zamawiający zastrzega sobie prawo do wniesienia uwag do treści dokumentacji SZBI zgłaszanych w trakcie procedury odbiorowej.
10. System Zarządzania Bezpieczeństwem Informacji musi być zgodny z obowiązującymi wymaganiami prawnymi w tym zakresie.
11. Zamawiający zastrzega, że wszelkie błędy w przygotowanej dokumentacji świadczące o tym, że dokumentacja została przeniesiona z innej organizacji/instytucji będą podstawą do odrzucenia dokumentów do poprawki, bez ich dalszej analizy ze strony Zamawiającego.
12. Opracowane polityki, procedury, instrukcje itd. muszą realnie odnosić się do zinwentaryzowanych wcześniej procesów Zamawiającego.
13. Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem

zrozumiałym dla osób nieposiadających wysokiego przygotowania w zakresie bezpieczeństwa informacji.

14. Dokumentacja SZBI powinna uwzględniać i obejmować obszary, o których mowa w § 19 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773)., w szczególności takie jak:
    1) polityka bezpieczeństwa informacji:
        a) polityki dotyczące bezpieczeństwa informacji,
        b) przegląd polityk bezpieczeństwa informacji,
    2) organizacja bezpieczeństwa informacji:
        a) role i odpowiedzialność za bezpieczeństwo informacji,
        b) rozdzielanie obowiązków,
        c) umowy z firmami trzecimi
        d) ankieta bezpieczeństwa dla firm trzecich
    3) zarządzanie aktywami:
        a) inwentaryzacja aktywów,
        b) użytkowania komputerów przenośnych,
        c) postępowanie z aktywami,
        d) zarządzanie nośnikami wymiennymi,
        e) postępowanie z nośnikami danych, naprawy i likwidacja sprzętu
    4) kontrola dostępu:
        a) polityka kontroli dostępu,
        b) dostęp do sieci i usług sieciowych,
        c) rejestrowanie i wyrejestrowywanie użytkowników,
        d) nadawanie, zmiana uprawnień i dostępów oraz zarządzanie kontem,
        e) zarządzanie prawami uprzywilejowanego dostępu,
        f) zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników,
        g) przegląd praw dostępu użytkowników,
        h) odbieranie lub dostosowywanie praw dostępu,
        i) stosowanie poufnych informacji uwierzytelniających,
        j) ograniczanie dostępu do informacji,
        k) procedury bezpieczeństwa logowania,
        l) system zarządzania hasłami
        m) użycie uprzywilejowanych programów narzędziowych,
        n) zdalny dostęp,
    5) kryptografia:
        a) polityka stosowania zabezpieczeń kryptograficznych,
        b) zarządzanie kluczami,
    6) bezpieczeństwo fizyczne i środowiskowe:
        a) fizyczna granica obszaru bezpiecznego,
        b) ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
        c) praca w obszarach bezpiecznych,
        d) dostawy,
        e) lokalizacja i ochrona sprzętu,
        f) konserwacja sprzętu,
        g) bezpieczne zbywanie lub przekazywanie do ponownego użycia,
        h) polityka czystego biurka i ekranu,

i) polityka kluczy,

7) bezpieczna eksploatacja:
   a) dokumentowanie procedur eksploatacyjnych,
   b) rozpoczęcie, zawieszenie i zakończenie pracy w systemie,
   c) zabezpieczenia przed szkodliwym oprogramowaniem,
   d) tworzenie kopii zapasowych i archiwizacja danych,
   e) rejestrowanie zdarzeń,
   f) rejestrowanie działań administratorów i operatorów,
   g) synchronizacja zegarów,
   h) instalacja oprogramowania w systemach produkcyjnych,
   i) zarządzanie podatnościami technicznymi,
   j) ograniczenia w instalowaniu oprogramowania,
8) bezpieczeństwo komunikacji:
   a) zabezpieczenia sieci,
   b) polityki i procedury przesyłania informacji,
   c) porozumienia dotyczące przesyłania informacji,
   d) wiadomości elektroniczne,
   e) weryfikacja zapisu umów z zewnętrznymi dostawcami w celu wdrażania
   f) odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa,
   g) zabezpieczanie usług aplikacyjnych w sieciach publicznych,
   h) outsourcing, współpraca ze stronami trzecimi,
9) zarządzanie incydentami związanymi z bezpieczeństwem informacji:
   a) odpowiedzialność i procedury,
   b) zgłaszanie zdarzeń związanych z bezpieczeństwem informacji,
   c) zgłaszanie słabości związanych z bezpieczeństwem informacji,
   d) ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem,
   e) reagowanie na incydenty związane z bezpieczeństwem informacji,
   f) wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji,
   g) gromadzenie materiału dowodowego,
   h) plan reagowania na incydenty
10) bezpieczeństwo informacji w zarządzaniu ciągłością działania:
   a) planowanie ciągłości bezpieczeństwa informacji,
   b) wdrożenie ciągłości bezpieczeństwa informacji,
11) zgodność:
   a) Przeglądy i aktualizacja dokumentacji SZBI.

Zadanie III: Przeprowadzenie analiz ryzyka oraz oceny skutków przetwarzania danych osobowych (DPIA).

1. W ramach usługi Wykonawca przeprowadzi analizę ryzyka oraz ocenę skutków dla przetwarzania danych (DPIA), w tym opracuje i wdroży metodykę szacowania ryzyka dla infrastruktury informatycznej i zinwentaryzowanych systemów oraz procesów przetwarzania danych osobowych oraz opracuje dokumentację opisującą strategię zarządzania ryzykiem, a także metodologie oceny skutków dla przetwarzania danych osobowych (DPIA).

2. Wykonawca opracuje i przekaże Zamawiającemu narzędzia do automatyzacji analizy ryzyka na podstawie opracowanej i przyjętej metodologii. Narzędzie musi być przejrzyste, zrozumiałe dla kierowników komórek organizacyjnych celem oszacowania ryzyka u Zamawiającego. Narzędzie musi uwzględniać wszelkie możliwe ryzyka, w tym wynikające z ustawy o cyberbezpieczeństwie.
3. Dokumentacja powinna zawierać m. in. takie informacje jak:
   1) identyfikacja ryzyk,
   2) rejestr ryzyk,
   3) kategoryzacja ryzyk
   4) Identyfikacja aktywów i procesów,
   5) Identyfikacja zagrożeń,
   6) Identyfikacja zabezpieczeń,
   7) Identyfikacja i ocena podatności, które mogą być wykorzystane i stanowić zagrożenia dla aktywów;
   8) Identyfikacja i ocena skutków utraty poufności, integralności i dostępności w odniesieniu do aktywów;
   9) Ocena ryzyka,
   10) Szacowanie ryzyka – w tym zaproponowanie metody szacowania ryzyka,
   11) Instruktaż dla pracowników Zamawiającego zaangażowanych w analizę ryzyka.
4. Wykonawca dokona wskazania obszarów wymagających dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagań do wdrożenia.
5. Wykonawca dokona identyfikacji zasobów krytycznych: lista kluczowych procesów, systemów i zasobów, które muszą być chronione.

Zadanie IV: Przeprowadzenie szkoleń dla pracowników i kadry kierowniczej oraz szkoleń specjalistycznych dla pracowników IT:

Szkolenia muszą być przeprowadzone przez osobę lub osoby posiadające stosowną wiedzę i minimum 2 letnie doświadczenie w przygotowywaniu i przeprowadzaniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

Szkolenia dla pracowników Zamawiającego:

1. Głównym tematem szkolenia ma być uświadomienie pracowników Zamawiającego o zagrożeniach w cyberprzestrzeni związanych z pracą na stanowisku komputerowym oraz dostępem do sieci Internet.
2. Minimalna wymagana tematyka szkolenia:
   1) metody ataków, w tym m.in. phishing, ransomware oraz malware i sposoby przeciwdziałania oraz zabezpieczania się przed tymi zagrożeniami,
   2) konsekwencje, jakie mogą ze sobą nieść nieuwaga i nieznajomość tych metod,
   3) bezpieczeństwo fizyczne,
   4) bezpieczeństwo pracy online,
   5) bezpieczna praca zdalna,
   6) socjotechnika,
   7) bezpieczeństwo haseł,
   8) bezpieczeństwo poczty e-mail i ochrona przed scam-em,

9) bezpieczeństwo stron www i przeglądarek,
10) ataki za pośrednictwem telefonu, zagrożenia związane z urządzeniami mobilnymi,
11) zagrożenia związane z sieciami wi-fi,
12) zagrożenia w mediach społecznościowych,
13) dobre praktyki bezpieczeństwa,
14) Identyfikowanie zagrożeń – przestrzeganie zasad bezpieczeństwa,
15) prywatność, poufność i anonimowość w internecie,
16) szyfrowanie dokumentów i poczty elektronicznej,
17) jak bezpiecznie przetwarzać dane (szyfrowanie, przechowywanie, udostępnianie),
18) wycieki danych w ostatnich latach (przykłady)
19) reakcje na incydenty bezpieczeństwa i naruszenia ochrony danych osobowych - odpowiedzialność i obowiązki pracowników.
20) wymagania i obowiązki dla pracowników wynikające z wdrożonej dokumentacji SZBI i wewnętrznych procedur w obszarze bezpieczeństwa informacji w tym danych osobowych.
21) podsumowanie szkolenia: odpowiedzi na pytania uczestników szkolenia.

3. Wymagania dotyczące szkolenia:
   1) czas trwania szkolenia: zalecany min. 3 godziny zegarowe,
   2) szkolenie na miejscu w siedzibie Zamawiającego, Zamawiający zapewnia salę,
   3) certyfikat ukończenia szkolenia,
   4) przewidywana liczba uczestników: do. 130 osób, w grupach po około 40 osób. Ostateczna liczba osób zostanie wskazana Wykonawcy na 2 dni robocze przed ustalonym terminem szkolenia.

Szkolenia dla kadry kierowniczej Zamawiającego:

1. Głównym tematem stacjonarnego szkolenia ma być uświadomienie kadry kierowniczej o obowiązkach ciążących na osobach zajmujących stanowiska kierownicze u Zamawiającego wynikających z przepisów prawa, omówienie zagrożeń w cyberprzestrzeni związanych z pracą na stanowisku komputerowym oraz dostępem do sieci Internet z uwzględnieniem obowiązków i odpowiedzialności kadry kierowniczej.
2. Proponowana tematyka szkolenia:
   1) System Zarządzania Bezpieczeństwem Informacji w praktyce,
   2) System Zarządzania Ciągłością Działania – dlaczego jest istotny i jak działa u Zamawiającego,
   3) odpowiedzialność członków organów kierowniczych w obszarze cyberbezpieczeństwa,
   4) Zarządzanie ryzykiem w bezpieczeństwie informacji,
   5) główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika,
   6) podstawowe przepisy prawa z zakresu ochrony danych i bezpieczeństwa informacji,
   7) wymagania i obowiązki dla kierowników wynikające z wdrożonej dokumentacji SZBI i wewnętrznych procedur w obszarze bezpieczeństwa informacji w tym danych osobowych.
   8) podsumowanie szkolenia: odpowiedzi na pytania uczestników szkolenia.
3. Proponowana tematyka szkolenia dla kadry kierowniczej powinna zostać rozszerzona o zagadnienia szkoleniowe przewidziane dla pracowników Zamawiającego.
4. Wymagania dotyczące szkolenia:
   5) czas trwania szkolenia: zalecany min. 5 godzin zegarowych,
   6) szkolenie na miejscu w siedzibie Zamawiającego, Zamawiający zapewnia salę,

7) certyfikat ukończenia szkolenia,
8) przewidywana liczba uczestników: do. 30 osób. Ostateczna liczba osób zostanie wskazana Wykonawcy na 2 dni robocze przed ustalonym terminem szkolenia.

Szkolenia specjalistyczne dla pracowników IT:

1. Ponadto Wykonawca zorganizuje i przeprowadzi szkolenia specjalistyczne dla pracowników IT, o tematyce związanej z:
   1) Zarządzanie usługą Active Directory w środowisku Microsoft Windows Server 2022 lub 2025, w tym:
      a) Instalacja i konfiguracja kontrolerów domeny;
         – Omówienie usług AD DS.
         – Omówienie kontrolerów domeny usług AD DS.
         – Wdrożenie kontrolera domeny
         – Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server
      b) Zarządzanie obiektami w AD DS.;
         – Zarządzanie kontami użytkowników
         – Zarządzanie grupami w usługach AD DS.
         – Zarządzanie obiektami typu komputer w AD DS.
         – Wdrażanie i zarządzanie OU
      c) Zarządzanie zaawansowaną infrastrukturą AD DS.;
         – Wprowadzenie do zaawansowanych wdrożeń AD DS.
         – Wdrożenie rozproszonego środowiska AD DS.
         – Konfiguracja relacji zaufania AD DS
      d) Wdrażanie i zarządzanie lokacjami i repliką AD DS.;
         – Omówienie replikacji usług AD DS.
         – Konfigurowanie lokacji usług AD DS.
         – Konfigurowanie i monitorowanie replikacji usług AD DS
      e) Wdrażanie zasad grupy;
         – Wprowadzenie do zasad grupy
         – Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)
         – Konfiguracja zakresu i przetwarzania obiektów GPO
         – Rozwiązywanie problemów z GPO
      f) Zarządzanie ustawieniami użytkowników za pomocą zasad grupy.
         – Wdrażanie szablonów administracyjnych
         – Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
         – Konfiguracja preferencji zasad grupowych

   2) Wirtualizacja Hyper-V, magazynowanie i przetwarzanie danych w środowisku Microsoft Windows Server 2022 lub 2025, w tym:
      a) Omówienie funkcji administracyjnych systemu Windows Server;
         – Informacje wstępne o systemie Windows Server
         – Omówienie najważniejszych funkcji systemu Windows Server
         – Omówienie zasad i narzędzi związanych z zarządzaniem systemem Windows Server
      b) Zarządzanie serwerami plików i pamięcią masową w systemie Windows Server;
         – Wolumeny i systemy plików w systemie Windows Server

- Współużytkowanie zasobów w systemie Windows Server
- Wdrażanie obszarów pamięci masowej w systemie Windows Server
- Wdrażanie funkcji deduplikacji danych
- Wdrażanie protokołu iSCSI
- Wdrażanie rozproszonego systemu plików
- Migracja magazynu danych w Windows Server

c) Oprogramowanie do wirtualizacji Hyper-V i kontenery w systemie Windows Server
- Hyper-V w systemie Windows Server
- Konfigurowanie maszyn wirtualnych
- Zabezpieczenie wirtualizacji w systemie Windows Server
- Ulepszenia działania wirtualnego przełącznika sieciowego w Windows Server
- Kontenery w systemie Windows Server

d) Funkcje wysokiej dostępności w systemie Windows Server;
- Planowanie wdrażania klastrów na potrzeby przełączania awaryjnego
- Tworzenie i konfigurowanie klastra przełączania awaryjnego
- Omówienie klastrów rozległych
- Funkcje wysokiej dostępności i rozwiązania do usuwania skutków awarii oparte na maszynach wirtualnych Hyper-V

e) Usuwanie skutków awarii w systemie Windows Server;
- Funkcja Hyper-V Replica
- Infrastruktura tworzenia i odtwarzania kopii zapasowych w systemie Windows Server

f) Implementowanie i zarządzanie zasobami typu failover clustering;
- Planowanie strategii wdrożenia typu failover cluster
- Tworzenie i konfiguracja struktury failover cluster
- Monitoring infrastruktury

g) Implementowanie rozwiązań typu failover clustering dla maszyn wirtualnych w Hyper-V;
- Prezentacja i integracja Hyper-V w Windows Server wraz z failover clustering
- Implementacja i zarządzanie maszynami wirtualnymi w Hyper-V w failover clusters
- Główne cechy wdrożeń maszyn wirtualnych w środowisku typu wysokiej dostępności i niezawodności
- Szyfrowane Cluster Shared Volumes w Windows Server

h) Implementowanie network load balancing.
- Przegląd metod zastosowania klastrów typu NLB
- Konfiguracja klastrów NLB
- Planowanie i implementacja NLB

2. Wymagania dotyczące szkolenia dla pracowników IT:
   1) forma i miejsce szkolenia: do indywidualnego ustalenia z Zamawiającym,
   2) certyfikat ukończenia szkolenia,
   3) przewidywana liczba uczestników: 2 osoby.

Założenia ogólne do szkoleń dla pracowników i kadry kierowniczej:

1. Szkolenia muszą być dedykowane dla JST i przeprowadzone przez osobę lub osoby posiadające stosowną wiedzę i minimum 2 letnie doświadczenie w przygotowywaniu

i przeprowadzaniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

2. Wymagania dotyczące szkoleń:
   1) Wykonawca dostarczy do akceptacji Zamawiającemu programy szkoleń dla pracowników, kadry kierowniczej oraz pracowników IT,
   2) Programy szkoleń szkolenia dla pracowników i kadry kierowniczej powinny obejmować wymogi dla Zamawiającego oraz obowiązki dla pracowników i kadry kierowniczej wynikające z:
      a) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie Cyberbezpieczeństwa;
      b) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
      c) Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
      d) Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
      e) 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;
      f) 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 (RODO);
      g) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (DODO);
      h) 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);
      i) Norm ISO, a w szczególności PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO 22301 oraz PN-EN ISO 22313;
      j) Narodowych Standardów Cyberbezpieczeństwa (NSC).
3. Wykonawca dokona zapisu (nagrania) audiowizualnego szkoleń i udostępni je po szkoleniu Zamawiającemu w celach wewnętrznych Zamawiającego, tj. w celach dalszego podnoszenia świadomości pracowników, w szczególności nieobecnych podczas szkolenia.
4. Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników szkoleń w wersji papierowej, które zostaną przekazane Zamawiającemu, nie później niż w dniu rozpoczęcia szkolenia.
5. Materiały szkoleniowe zawierające treści z zakresu tematyki szkolenia, instrukcje, prezentacje, opisy ćwiczeń, opracowania graficzne, wykorzystywane w trakcie trwania szkolenia, zostaną sporządzone w języku polskim i będą obejmować teoretyczne oraz praktyczne aspekty zagadnień poruszanych w trakcie szkolenia i będą oparte na dokumentacji wdrożonej u Zamawiającego.
3. Potwierdzeniem wykonania szkoleń dla pracowników i kadry kierowniczej będą listy

obecności, które powinny zawierać następujące elementy:

1) Nagłówek: Nazwa projektu, tytuł szkolenia, data i miejsce szkolenia;
2) Dane uczestników: Imię i nazwisko;
3) Podpisy uczestników: Każdy uczestnik powinien podpisać się obok swojego nazwiska, potwierdzając swoją obecność;
4) Godziny szkolenia: Czas rozpoczęcia i zakończenia szkolenia;
5) Dane prowadzącego: Imię i nazwisko osoby prowadzącej szkolenie;
6) Uwagi: Miejsce na ewentualne uwagi dotyczące szkolenia.

4. Na papierowej wersji listy obecności powinny znajdować się loga związane z projektem, takie jak logo inicjatywy „Cyberbezpieczny Samorząd".
5. Wykonawca wystawi certyfikaty potwierdzające uczestnictwo w szkoleniu dla każdego uczestnika szkolenia.

Zadanie V: Wykonanie testów bezpieczeństwa i podatności.

1. Testy bezpieczeństwa i podatności powinny obejmować:
   a) Analizę usług oraz zasobów publicznie dostępnych w sieci Internet, w tym:
      – Ocena podatności na ataki: wykonanie skanowania pod względem podatności i oceny zgodności z najlepszymi praktykami zabezpieczeń.
      – Urządzenia brzegowe: Sprawdzenie konfiguracji firewalli, IPS/IDS, mechanizmów anty DDoS oraz zabezpieczeń SSL/TLS.
   b) Analizę bezpieczeństwa poczty elektronicznej, w tym:
      – Weryfikacja poprawności konfiguracji mechanizmów SPF, DMARC, DKIM.
      – Szyfrowanie poczty: Ocena implementacji szyfrowania (S/MIME, PGP), bezpieczne przechowywanie i zarządzanie kluczami.
   c) Analizę Bezpieczeństwa infrastruktury sieciowej, w tym:
      – Konfiguracja urządzeń sieciowych: Szczegółowa analiza konfiguracji firewalli, routerów, przełączników oraz punktów dostępowych, ocena segmentacji sieci i VLAN.
      – Analiza bezpieczeństwa sieci wewnętrznych i zewnętrznych, ocena bezpieczeństwa VPN.
   d) Analizę udostępnionych usług wraz z testami bezpieczeństwa mającymi na celu weryfikację istnienia podatności na ataki sieciowe.
   e) Analizę bezpieczeństwa infrastruktury sprzętowej i oprogramowania, w tym:
      – weryfikacja aktualizacji systemów operacyjnych, aplikacji, firmware urządzeń.
      – ocena weryfikacja wdrożonych polityk bezpieczeństwa oraz zarządzania zasobami IT pod względem stosowania bezpiecznych praktyk administracyjnych.
   f) Analizę bezpiecznej konfiguracji domeny Microsoft Active Directory, w tym:
      – weryfikacja poprawnej konfiguracji domeny oraz wdrożonych polityk bezpieczeństwa wraz z oceną zabezpieczeń Kerberos I analizą polityki haseł.
      – Weryfikacja GPO (Group Policy Objects), audyt uprawnień użytkowników i grup, analiza logowania i monitorowania zdarzeń.
   g) Analizę bezpieczeństwa aplikacji, w tym:
      – Aplikacje utrzymywane w sieci wewnętrznej zostaną poddane analizie, której celem jest określenie stopnia podatności na ataki.

- W zależności od rodzaju aplikacji występujących w środowisku klienta, zastosowane zostaną dopasowane techniki pozwalające na wykrycie luk oraz błędów w obszarach związanych z daną usługą, w tym zostanie przeprowadzona weryfikacja konfiguracji baz danych, ocena mechanizmów autoryzacji i uwierzytelnienia pod względem podatności na ataki.

h) Analizę bezpieczeństwa danych – backupy, w tym:
   - Ocena polityki backupów w organizacji, w tym częstotliwości tworzenia kopii zapasowych i ich przechowywania.
   - Weryfikacja zgodności procedur backupowych z przyjętymi standardami branżowymi.
   - Sprawdzenie czy kopie zapasowe przechowywane są w odseparowanych, bezpiecznych i oddzielnych lokalizacjach.
   - Weryfikacja szyfrowania kopii zapasowych w celu ochrony przed nieautoryzowanym dostępem.

i) Weryfikację poprawności aktualnej dokumentacji, w tym sprawdzenie czy dokumentacja dotycząca bezpieczeństwa jest kompletna i zgodna z obowiązującymi standardami.

j) Wykonanie testów socjotechnicznych, taki jak np.:
   - Przeprowadzenie symulowanych ataków phishingowych, ocena wyników i opracowanie rekomendacji na podstawie zachowań pracowników.
   - Kampania zostanie podzielona na trzy grupy odbiorców, aby ocenić różne poziomy wrażliwości i odpowiedzi na tego typu zagrożenia.
   - Szczegółowe wymagania do przeprowadzenia testów socjotechnicznych:
     - Wykonawca będzie zobowiązany do zachowania poufności i przestrzegania przepisów o ochronie danych osobowych oraz do prowadzenia audytu w sposób uczciwy i obiektywny.
     - Przygotowanie co najmniej 3 zdefiniowanych scenariuszy ataków, na podstawie przekazanych przez Zamawiającego informacji (podejrzane wiadomości e-mail).
     - Dostosowanie przygotowanych scenariuszy do specyfiki Zamawiającego (wspólne uzgodnienie z Zamawiającym).
     - Przeprowadzenie co najmniej 6 ataków socjotechnicznych mających na celu wyłudzenie poufnych informacji lub uzyskanie nieautoryzowanego dostępu do systemów Zamawiającego poprzez manipulację i wykorzystanie ludzkiego czynnika jako wektora ataku.
     - W przypadku skuteczności ataku analizę danych i informacji w skrzynkach pocztowych takich pracowników celem określenia ich przydatności do dalszej eskalacji ataku.
     - Zamawiający wyraża zgodę na wykorzystanie wizerunku Zamawiającego w tym w szczególności: logo, nazwy domeny i grafiki, stopki podpisu wiadomości.

2. Zamawiający wymaga przygotowania raportu z realizacji Zadania V zawierającego:
   a) szczegółowe wyniki wizji lokalnej,
   b) podkreślenie obszarów wymagających uwagi oraz punktów mocnych w zabezpieczeniach fizycznych,
   c) wykaz konkretnych podatności, wraz z nazwami, numerami CVE (Common Vulnerabilities and Exposures) oraz opisami. Kategorie podatności, takie jak ataki

XSS, SQL injection, itp.

d) kopie zrzutów ekranu, logów czy innych danych wspierających identyfikację podatności,
e) wskazanie, ile podatności zostało sklasyfikowanych jako niskie, średnie, wysokie i krytyczne,
f) opis, jakie mogą być skutki wykorzystania danej podatności (utraty danych, przerwy w dostępie, ataki hakerskie),
g) przedstawienie możliwych scenariuszy ataku, które wykorzystują zidentyfikowane podatności,
h) wskazanie, które podatności powinny być naprawione jako pierwsze, bazując na ich krytyczności i potencjalnych skutkach,
i) opis użytych narzędzi do skanowania podatności oraz metodyki przeprowadzenia skanowania,
j) wskazanie, jakie należy podjąć działania, aby zlikwidować lub zminimalizować skutki każdej zidentyfikowanej podatności,
k) określenie rekomendowanych terminów naprawy dla poszczególnych podatności,
l) informacje na temat warunków, w jakich skanowanie zostało przeprowadzone.

3. Zamawiający wymaga aby Wykonawca dołożył wszelkich starań, aby w trakcie realizacji zadania V nie zakłócać normalnego funkcjonowania Urzędu.
4. Zamawiający nie dopuszcza wykonania Zadania V w sposób zdalny. Badanie zabezpieczeń, podatności systemów, przeprowadzenie testów bezpieczeństwa i podatności Wykonawca powinien wykonać w obiektach Zamawiającego.
5. Zamawiający wymaga, aby Wykonawca wykazał, że dysponuje lub będzie dysponował przynajmniej jednym specjalistą ds. bezpieczeństwa IT, posiadającym minimum jeden z następujących certyfikatów: Certified Ethical Hacker (CEH), Certified Penetration Testing Engineer (CPTE), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE).

Usługi będące przedmiotem umowy powinny być świadczone w oparciu o przepisy normy i wymagania zawarte m.in. w :

1. Rozporządzeniu 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;
2. Ustawie z dnia 5 lipca 2018 r. o krajowym systemie Cyberbezpieczeństwa;
3. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych;
4. Rozporządzeniu 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 (RODO);
5. Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w

sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (DODO);

6. Dyrektywie 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);
7. Normie ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
8. Narodowych Standardach Cyberbezpieczeństwa (NSC).
9. Wytycznych i innych dokumentach wymienionych w Regulaminie Konkursu Grantowego Cyberbezpieczny Samorząd.

Okres realizacji zamówienia: 170 dni kalendarzowych od daty podpisania umowy.