Znak sprawy: PPF.042.16.6.2024
Dokument: Załącznik nr 1 – opis przedmiotu zamówienia
Garwolin, dn. 18.03.2025 r.

OPIS PRZEDMIPOTU ZAMÓWIENIA

Zadanie 1: Przeprowadzenie audytu systemu zarządzania bezpieczeństwem informacji wraz z usługą testów penetracyjnych, wydaniem i omówieniem raportów z kadrą kierowniczą Urzędu.

Audyt bezpieczeństwa informacji obejmuje wszystkie obszary funkcjonowania Zamawiającego:

1. **Audyt organizacyjny:**
   1.1. weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
   1.2. odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
   1.3. dokumentacja, w tym z zakresu ochrony danych osobowych;
   1.4. analiza ryzyka;
   1.5. inwentaryzacja aktywów;
   1.6. plan postępowania z ryzykiem;
   1.7. przeprowadzenie wywiadów z wybranymi pracownikami.
2. **Audyt fizyczny i środowiskowy**
   2.1. weryfikacja zabezpieczeń wejścia/wyjścia;
   2.2. weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;
   2.3. weryfikacja bezpieczeństwa okablowania strukturalnego;
   2.4. weryfikacja systemów chłodzenia i systemów alarmowych.
3. **Audyt teleinformatyczny**
   3.1. przeprowadzenie testów penetracyjnych systemu informatycznego wewnętrznie i zewnętrznie, określenie luk, wskazanie rozwiązań naprawczych, opracowanie raportu;
   3.2. weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi;
   3.3. przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania i ciągłości działania;
   3.4. weryfikacja ochrony przed oprogramowaniem szkodliwym;
   3.5. weryfikacja procedur zarządzania kopiami zapasowymi;
   3.6. weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
   3.7. weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
   3.8. weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
   3.9. Analiza i ocena mechanizmów zarządzania oraz ich aktualizacja.

Wymagania w zakresie przeprowadzonego audytu.

1. Zamawiający wymaga, aby audyty zostały przeprowadzone w zgodzie z Krajowymi Ramami Interoperacyjności (KRI) z uwzględnieniem elementów ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) w kontekście Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
2. Zamawiający wymaga, aby na zespole audytorskim Wykonawcy spoczywał obowiązek weryfikacji zgodności z innymi przepisami, w tym:

2.1. zgodność z przepisami dotyczącymi ochrony danych osobowych (np. RODO), w kontekście zarządzania danymi, bezpieczeństwa informacji oraz cyberbezpieczeństwa;
2.2. sprawdzenie zgodności z krajowymi i międzynarodowymi normami oraz standardami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.
2.3. Audyt SZBI stanowi kluczowy element w ramach projektu Cyberbezpieczny Samorząd, a jego celem jest dokonanie oceny obecnego stanu bezpieczeństwa informacji u Zamawiającego, w tym identyfikacja wszelkich zagrożeń, słabości, luk w zabezpieczeniach itd.
3. Na podstawie wyników audytu należy zweryfikować braki i obszary wymagające poprawy, co kluczowe jest dla skutecznego wdrożenia działań w ramach projektu. Audyt niezbędny jest dla Zamawiającego do oceny zgodności z normami i standardami dotyczącymi zarządzania bezpieczeństwem informacji, a jego wyniki stanowią fundament do opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
4. Zamawiający wymaga, aby audyty przeprowadzone zostały przez zespół audytorski stacjonarnie, w siedzibie Zamawiającego tj. Urzędzie Miasta Garwolin.
5. Zamawiający wymaga, aby w ramach czynności audytowych Wykonawca przeprowadził kompleksowe testy penetracyjne (wraz z czynnościami audytowymi) infrastruktury IT Urzędu Miasta Garwolin. Testy penetracyjne mają na celu identyfikację i ocenę nieznanych dotąd podatności. Testy te muszą być wykonane przez wykwalifikowanego pentestera i powinny obejmować szczegółową analizę zarówno zewnętrznych, jak i wewnętrznych komponentów systemu informatycznego.
6. Zamawiający wymaga, aby zakres testów penetracyjnych obejmował m.in.:
6.1. Zewnętrzne testy penetracyjne infrastruktury IT:
6.2. analiza topologii sieci na granicy z Internetem - szczegółowe zbadanie struktury sieci na styku z Internetem, z uwzględnieniem istniejących zabezpieczeń;
6.2.1. ocena mechanizmów ochronnych - sprawdzenie efektywności systemów zabezpieczeń, takich jak zapory sieciowe, IDS/IPS oraz inne urządzenia na granicy sieci;
6.2.2. wykrywanie publicznie dostępnych usług sieciowych - przeprowadzenie skanowania portów oraz usług dostępnych publicznie w celu zidentyfikowania potencjalnych punktów dostępu dla atakujących;
6.2.3. identyfikacja wersji i typów publicznie dostępnego oprogramowania - ustalenie wersji oprogramowania, które jest widoczne z sieci publicznej, w celu określenia możliwych luk w zabezpieczeniach;
6.2.4. próby wykorzystania wykrytych podatności - testowanie ryzyka poprzez wykorzystanie zidentyfikowanych luk bezpieczeństwa;
6.2.5. zalecenia dotyczące wzmocnienia ochrony sieci brzegowej - przygotowanie zaleceń dotyczących wzmocnienia ochrony na granicy sieci lokalnej z Internetem.
7. **Wewnętrzne testy penetracyjne infrastruktury IT:**
7.1. ocena struktury sieci LAN: Szczegółowa analiza wewnętrznej topologii sieci LAN, w tym rozmieszczenia urządzeń oraz zastosowanych mechanizmów ochrony;
7.2. testowanie wewnętrznych zabezpieczeń sieciowych - sprawdzenie izolacji urządzeń, segmentacji sieci oraz innych środków ochronnych stosowanych w sieci wewnętrznej;
7.3. analiza i monitoring ruchu sieciowego - przeprowadzenie dokładnego monitoringu ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących świadczyć o naruszeniu bezpieczeństwa;
7.4. skanowanie portów i usług w sieci LAN - identyfikacja usług i aplikacji działających w sieci wewnętrznej poprzez skanowanie portów TCP/UDP;
7.5. wykrywanie aktywnych urządzeń w sieci - identyfikacja i analiza urządzeń podłączonych do sieci lokalnej w celu oceny potencjalnych zagrożeń;
7.6. eksploatacja zidentyfikowanych podatności w sieci LAN - przeprowadzenie prób wykorzystania słabości w sieci wewnętrznej w celu oceny ryzyka;
7.7. ocena procedur tworzenia i odzyskiwania kopii zapasowych - przegląd skuteczności procedur backupu i przywracania danych;

7.8. rekomendacje dla poprawy bezpieczeństwa wewnętrznej sieci LAN - przygotowanie szczegółowych zaleceń dotyczących zwiększenia poziomu zabezpieczeń sieci lokalnej.

8. Audyt bezpieczeństwa serwisów WWW:

8.1. sprawdzenie aktualności serwera HTTP oraz systemu CMS - ocena zgodności wersji oprogramowania serwerowego oraz systemu CMS z najnowszymi standardami bezpieczeństwa, z naciskiem na wykrywanie znanych luk;

8.2. ocena bezpieczeństwa komunikacji internetowej - analiza stosowanych certyfikatów X.509, wersji protokołu TLS oraz metod kryptograficznych, zapewniających poufność i integralność transmisji danych przez Internet.

9. Audyt bezpieczeństwa serwisów pocztowych:

9.1. analiza mechanizmów SPF, DKIM i DMARC - ocena poprawności implementacji mechanizmów SPF, DKIM oraz DMARC, mających na celu ochronę przed fałszerstwami wiadomości e-mail;

9.2. ocena zabezpieczeń TLS w komunikacji e-mailowej - sprawdzenie czy mechanizmy szyfrowania TLS zostały poprawnie wdrożone w celu zabezpieczenia komunikacji pocztowej.

10. Raport z przeprowadzonych testów i audytów:

10.1. dokumentacja wykonanych prac - szczegółowy raport zawierający opis zastosowanej metodologii, użytych narzędzi oraz zakresu wykonanych testów i analiz;

10.2. analiza wyników testów penetracyjnych - przedstawienie wyników testów, wraz z identyfikacją wykrytych podatności i oceną związanego z nimi ryzyka;

10.3. zalecenia i wnioski - opracowanie rekomendacji dotyczących naprawy wykrytych problemów oraz strategii mających na celu podniesienie poziomu bezpieczeństwa;

10.4. szczegółowa analiza technicznych zabezpieczeń - ocena oraz omówienie stanu zabezpieczeń serwisów WWW, serwisów pocztowych, sieci LAN i połączeń z Internetem, wraz z zaleceniami dotyczącymi utrzymania wysokiego poziomu bezpieczeństwa.

Niniejszy opis przedstawia minimalny zakres wymagań dla przeprowadzenia kompleksowych testów penetracyjnych oraz audytów bezpieczeństwa IT, które mają na celu wszechstronną ocenę stanu bezpieczeństwa informatycznego Urzędu Miasta Garwolin.

Wykaz certyfikatów, które powinien posiadać Wykonawca:

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 2016r. 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.

Zadanie 2: Opracowanie nowych polityk i procedur oraz aktualizacja posiadanej dokumentacji w ramach opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji (dalej SZBI) w Urzędzie Miasta Garwolina.

1. Zamawiający wymaga od Wykonawcy analizy i aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Garwolin wraz ze szczegółową aktualizacją, (ewentualnym opracowaniem w przypadku stwierdzenia braków) i wdrożeniem planów i procedur.
2. Zamawiający wymaga następującego zakresu prac:
   - **2.1.** Analiza i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):
     - **2.1.1.** przegląd zgodności dokumentacji z przepisami prawa – dokładna analiza obowiązujących w Urzędzie procedur, polityk i regulacji wewnętrznych dotyczących zarządzania bezpieczeństwem informacji. Weryfikacja, czy dokumentacja SZBI jest zgodna z aktualnymi wymaganiami wynikającymi z przepisów prawa krajowego i międzynarodowego, w tym przepisami RODO, Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UoKSC) oraz Dyrektywę NIS2;
     - **2.1.2.** ocena adekwatności obecnych procedur – przegląd obecnych procedur w kontekście ich aktualności i zastosowania w praktyce. Identyfikacja luk w dokumentacji, przestarzałych procesów, które mogą nie odpowiadać obecnym zagrożeniom cybernetycznym, oraz niespójności w dokumentacji SZBI;
     - **2.1.3.** analiza procesów zarządzania ryzykiem – sprawdzenie, czy obecne procesy identyfikacji, oceny i zarządzania ryzykiem są dostosowane do zmieniającego się krajobrazu zagrożeń i technologii. Opracowanie zaleceń dotyczących aktualizacji tych procesów w celu lepszego zabezpieczenia danych i systemów Urzędu przed nowymi zagrożeniami;
     - **2.1.4.** weryfikacja integracji z systemami IT - sprawdzenie czy dokumentacja SZBI jest odpowiednio zintegrowana z istniejącymi systemami IT w Urzędzie, w tym systemami do zarządzania tożsamością, ochrony danych osobowych, a także systemami monitorowania i analizy zagrożeń (SIEM). Ocenie zostanie poddane także, czy dokumentacja przewiduje odpowiednie mechanizmy ochrony informacji w różnych obszarach IT, w tym ochronę dostępu do systemów, szyfrowanie danych oraz zarządzanie kluczami szyfrującymi.
3. **Aktualizacja dokumentacji SZBI:**
   - **3.1.** dostosowanie dokumentacji do nowych wymagań – opracowanie zaktualizowanych procedur i polityk bezpieczeństwa, uwzględniających nowe zagrożenia, zmieniające się przepisy prawa oraz wymagania wynikające z międzynarodowych norm, takich jak ISO/IEC 27001 i NIS2. Nowe wersje dokumentacji będą zawierały aktualne procedury postępowania z incydentami, zarządzania ryzykiem, ochrony danych osobowych i kontroli dostępu.
   - **3.2.** aktualizacja polityk klasyfikacji i ochrony danych – wprowadzenie nowych zasad dotyczących klasyfikacji danych, zapewniających ich ochronę w zależności od poziomu wrażliwości. Polityki te obejmą zarządzanie dostępem, szyfrowanie, a także procesy bezpiecznego przetwarzania danych, zgodnie z wymogami RODO;
   - **3.3.** integracja z procedurami zarządzania incydentami – zapewnienie, że nowe procedury zarządzania incydentami, opracowane w ramach tego zamówienia, zostaną odpowiednio zintegrowane z dokumentacją SZBI, tworząc spójny system zarządzania bezpieczeństwem informacji, w którym wszelkie incydenty są skutecznie monitorowane, zgłaszane i rozwiązywane zgodnie z ustalonymi procedurami;
   - **3.4.** dostosowanie dokumentacji do nowoczesnych narzędzi zarządzania - aktualizacja dokumentacji w taki sposób, aby była kompatybilna z narzędziami i systemami wykorzystywanymi przez Urząd, w tym z systemami do monitorowania zagrożeń,

systemami zarządzania tożsamością i kontrolą dostępu, a także z oprogramowaniem SIEM i narzędziami do zarządzania incydentami.

4. **Weryfikacja istniejących planów i procedur reagowania na incydenty cybernetyczne:**
   - **4.1.** Przeprowadzenie dokładnego przeglądu obowiązujących procedur oraz planów reagowania na incydenty cybernetyczne w Urzędzie Miasta Garwolin pod kątem ich zgodności z aktualnymi standardami oraz skuteczności. Weryfikacja czy plany obejmują wszystkie istotne zagrożenia (np. ataki ransomware, phishing, naruszenia danych) i czy odpowiednio przewidują działania w przypadku różnych scenariuszy incydentów;
   - **4.2.** Weryfikacja zgodności z aktualnymi regulacjami prawnymi, w tym z RODO, Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UoKSC) oraz międzynarodowymi standardami, takimi jak ISO/IEC 27001:2023 czy dyrektywy NIS2.
   - **4.3.** Weryfikacja czy plany reagowania obejmują wszystkie wymagane rodzaje incydentów, w tym:
     - **4.3.1.** naruszenia ochrony danych osobowych;
     - **4.3.2.** ataki na systemy IT (np. ataki DdoS, phishing, ransomware);
     - **4.3.3.** nieautoryzowane dostępy do systemów i informacji.
     - **4.3.4.** identyfikacja braków, obszarów wymagających aktualizacji oraz zagrożeń, które mogą nie być obecnie wystarczająco adresowane przez istniejące procedury.
     - **4.3.5.** sporządzenie raportu z weryfikacji, który będzie stanowił podstawę do dalszych prac aktualizacyjnych.
     - **4.3.6.** opracowanie planów reagowania na incydenty o różnym poziomie zagrożenia- aktualizacja lub opracowanie nowych planów reagowania na incydenty, które będą uwzględniały różne poziomy zagrożeń (niski, średni, wysoki). Procedury powinny jasno określać, jakie działania należy podjąć w przypadku wykrycia incydentów cybernetycznych, w tym:
     - **4.3.7.** natychmiastowe działania zaradcze (np. izolacja zagrożonych systemów, powiadomienie odpowiednich organów, takie jak CERT Polska);
     - **4.3.8.** procedury przywracania systemów do pełnej sprawności;
     - **4.3.9.** zasady postępowania z danymi osobowymi i raportowania naruszeń zgodnie z RODO.
     - **4.3.10.** określenie procesów komunikacji wewnętrznej i zewnętrznej – uwzględnienie planów komunikacji wewnętrznej (w organizacji) oraz zewnętrznej (z mediami, interesariuszami, organami nadzoru). Komunikacja ta powinna być skoordynowana i zawierać odpowiednie procedury informowania o incydentach w sposób bezpieczny, zgodny z obowiązującymi regulacjami;
5. **Monitorowanie i wsparcie po wdrożeniu:**
   - **5.1.** monitorowanie działania procedur – zapewnienie wsparcia w monitorowaniu funkcjonowania wdrożonych planów i procedur przez okres co najmniej 6 miesięcy od ich wdrożenia. Monitoring powinien obejmować analizę skuteczności systemu zgłaszania incydentów oraz reakcję zespołu na rzeczywiste zdarzenia.
   - **5.2.** wprowadzenie korekt – na podstawie wyników monitoringu oraz zgłoszonych incydentów, wykonawca zobowiązany będzie wprowadzić niezbędne korekty w dokumentacji oraz procedurach, zapewniając ich dalsze dostosowanie do pojawiających się zagrożeń.

Zadanie 3: Aktualizacja, opracowanie i wdrożenie planów i procedur reagowania na incydenty cybernetyczne.

1. **Wdrożenie planów i procedur reagowania na incydenty cybernetyczne:**
   - **1.1.** wdrożenie planów i procedur w organizacji – przeprowadzenie pełnego wdrożenia zaktualizowanych planów reagowania na incydenty, obejmującego szkolenia dla pracowników oraz wytyczne dotyczące zgłaszania incydentów. Procedury te powinny być

dostosowane do codziennych zadań pracowników, a jednocześnie spełniać wymagania organów nadzoru;

1.2. symulacje i testy penetracyjne – przeprowadzenie symulacji incydentów oraz testów penetracyjnych w celu przetestowania wdrożonych procedur. Symulacje te powinny obejmować różne scenariusze incydentów cybernetycznych, takie jak ataki ransomware, próby phishingu, naruszenia ochrony danych osobowych, aby ocenić skuteczność systemu reagowania;

1.3. przygotowanie zespołu reagowania na incydenty (CSIRT) – w ramach wdrożenia, zespół reagowania na incydenty (CSIRT) zostanie odpowiednio przeszkolony w zakresie nowych procedur, zapewniając gotowość na różne zagrożenia i incydenty.

Zadanie 4: Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla wszystkich pracowników Urzędu z podziałem na kadrę zarządzającą i pozostałych pracowników z zakresu bezpieczeństwa informacji dla Urzędu

1. Zamawiający informuje, że celem usługi jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników oraz kady zarządzającej Zamawiającego, realizowanego w ramach Projektu Grantowego „Cyberbezpieczny Samorząd". Szkolenie to jest częścią Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC), Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

2. Zamawiający wymaga, aby podczas szkolenia przeprowadzonego w siedzibie Zamawiającego, w części teoretycznej poruszone zostały kluczowe aspekty cyberbezpieczeństwa, w tym m.in.:

2.1. Wprowadzenie do cyberbezpieczeństwa - definicja i znaczenie cyberbezpieczeństwa w administracji publicznej. Omówienie roli i odpowiedzialności pracowników w utrzymaniu bezpieczeństwa informacji.

2.2. Podstawowe zasady cyberbezpieczeństwa - omówienie fundamentalnych reguł i procedur dotyczących ochrony danych, zarządzania hasłami, autoryzacji i bezpiecznego korzystania z zasobów informatycznych.

2.3. Phishing i inne ataki socjotechniczne - rozpoznawanie i ochrona przed próbami wyłudzenia informacji, atakami phishingowymi oraz innymi technikami socjotechnicznymi.

2.4. Zagrożenia związane z oprogramowaniem typu ransomware i malware - identyfikacja, mechanizmy działania oraz metody zapobiegania i reagowania na zagrożenia związane z ransomware i malware.

2.5. Bezpieczna obsługa poczty elektronicznej - zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników oraz linków, a także ochrona przed spamem i phishingiem.

2.6. Zarządzanie hasłami i autoryzacja - tworzenie silnych haseł, korzystanie z menedżerów haseł, wprowadzenie autoryzacji dwuetapowej oraz znaczenie kluczy sprzętowych.

2.7. Ochrona urządzeń mobilnych - zabezpieczanie urządzeń przenośnych, takich jak smartfony
i tablety, przed utratą danych, kradzieżą oraz złośliwym oprogramowaniem.

2.8. Bezpieczne przetwarzanie i przechowywanie danych - szyfrowanie danych, zasady bezpiecznego przechowywania informacji, zarządzanie dostępem oraz udostępnianie danych w sposób bezpieczny.

2.9. Zarządzanie ryzykiem w cyberbezpieczeństwie - identyfikacja i ocena ryzyka, zarządzanie ryzykiem oraz wdrażanie odpowiednich środków zabezpieczających.

2.10. Ochrona przed spoofingiem i atakami telefonicznymi - mechanizmy ochrony przed spoofingiem, fałszowaniem numerów telefonów oraz innymi technikami oszustw telefonicznych.

2.11. **Zarządzanie dostępem do systemów i informacji** - zasady przydzielania uprawnień, kontrola dostępu oraz monitorowanie aktywności użytkowników w systemach informacyjnych.
2.12. **Bezpieczna komunikacja w środowisku cyfrowym -** szyfrowanie komunikacji, korzystanie z bezpiecznych kanałów komunikacyjnych, zabezpieczenie wideokonferencji oraz przesyłania danych.
2.13. **Ochrona przed wyłudzeniami danych osobowych (PII) -** zapobieganie wyłudzeniom danych osobowych za pomocą metod socjotechnicznych oraz przeciwdziałanie kradzieży tożsamości.
2.14. **Reagowanie na incydenty bezpieczeństwa -** procedury postępowania w przypadku incydentu, raportowanie naruszeń, analizowanie przyczyn oraz minimalizowanie skutków.
2.15. **Ochrona infrastruktury IT przed zagrożeniami -** zabezpieczenia techniczne, takie jak firewalle, systemy wykrywania włamań (IDS/IPS), aktualizacje i zarządzanie łatami bezpieczeństwa.
2.16. **Szkolenie w zakresie testów penetracyjnych i symulacji ataków** - ćwiczenia obejmujące symulacje rzeczywistych ataków na systemy informacyjne, testowanie odporności na zagrożenia oraz analiza wyników testów penetracyjnych.

3. Zamawiający wymaga, aby szkolenie zostało zaprojektowane w taki sposób, aby nie tylko podnosić świadomość w zakresie cyberbezpieczeństwa, ale także rozwijać praktyczne umiejętności uczestników w rozpoznawaniu i neutralizowaniu zagrożeń. Zakres tematyczny bloku szkoleniowego winien być zgodny z wymogami projektu i stanowić integralną część strategii podnoszenia poziomu ochrony informacji w administracji publicznej.
4. Zamawiający wymaga, aby podczas szkolenia dla kadry kierowniczej poruszone zostały kluczowe aspekty systemu w tym min.:
   4.1. Wprowadzenie do Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):
      4.1.1. definicja i znaczenie SZBI;
      4.1.2. podstawowe pojęcia związane z bezpieczeństwem informacji;
      4.1.3. przegląd normy ISO/IEC 27001:2023;
      4.1.4. kluczowe elementy SZBI i ich rola w organizacji;
   4.2. Polityka Bezpieczeństwa Informacji:
      4.2.1. definicja i cel Polityki Bezpieczeństwa Informacji;
      4.2.2. tworzenie, wdrażanie i utrzymanie polityki bezpieczeństwa;
      4.2.3. rola kadry kierowniczej w zarządzaniu polityką bezpieczeństwa;
   4.3. Zarządzanie ryzykiem:
      4.3.1. proces identyfikacji, analizy i oceny ryzyka;
      4.3.2. metodyka oceny ryzyka zgodnie z ISO/IEC 27005;
      4.3.3. implementacja i monitorowanie środków kontrolnych;
   4.4. Zarządzanie incydentami bezpieczeństwa:
      4.4.1. definicja incydentu bezpieczeństwa i jego rodzaje;
      4.4.2. procedury raportowania i reagowania na incydenty;
      4.4.3. role i odpowiedzialności w zarządzaniu incydentami;
      4.4.4. przykłady praktycznych scenariuszy incydentów;
   4.5. Kontrola dostępu i zarządzanie tożsamością:
      4.5.1. zasady kontroli dostępu w organizacji;
      4.5.2. bezpieczne zarządzanie tożsamością użytkowników;
      4.5.3. autoryzacja, autentykacja i monitorowanie aktywności;
   4.6. Świadomość i szkolenia pracowników:
      4.6.1. rola edukacji i szkoleń w zapewnieniu bezpieczeństwa informacji;
      4.6.2. tworzenie programu szkoleń z zakresu bezpieczeństwa informacji;
      4.6.3. praktyczne wskazówki dotyczące podnoszenia świadomości pracowników;

4.7. Audyt i monitorowanie systemu:
- **4.7.1.** procedury audytu wewnętrznego SZBI;
- **4.7.2.** monitorowanie i przegląd efektywności systemu;
- **4.7.3.** rola kadry kierowniczej w zapewnieniu zgodności z wymaganiami;

4.8. Zarządzanie ciągłością działania:
- **4.8.1.** planowanie i wdrażanie strategii ciągłości działania;
- **4.8.2.** testowanie i aktualizacja planów ciągłości;
- **4.8.3.** integracja zarządzania ciągłością działania z SZBI;

4.9. Przepisy prawne i regulacyjne:
- **4.9.1.** przegląd kluczowych przepisów prawa dotyczących ochrony danych i bezpieczeństwa informacji;
- **4.9.2.** obowiązki urzędów w zakresie zgodności z przepisami;
- **4.9.3.** zarządzanie zgodnością z RODO i innymi regulacjami;

4.10. Rola i odpowiedzialność kadry kierowniczej:
- **4.10.1.** kluczowe zadania kadry kierowniczej w zakresie zarządzania bezpieczeństwem informacji;
- **4.10.2.** budowanie kultury bezpieczeństwa w organizacji;
- **4.10.3.** motywowanie i nadzorowanie zespołów odpowiedzialnych za SZBI.

Wymagania w zakresie prowadzonych szkoleń.

1. Zakres szkolenia obejmuje aspekty teoretyczne i praktyczne z treścią i zawartością wdrożonej w dokumentacji SZBI w Urzędzie Miasta Garwolina z uwzględnieniem elementów zabezpieczeń infrastruktury IT.
2. Liczba uczestników i grup szkoleniowych:
2.1. Całkowita liczba uczestników: 73 pracowników.
2.2. Liczba grup szkoleniowych: Minimum 2-3 grupy aby uniknąć dezorganizacji normalnej pracy jednostki.
2.3. Podział na grupy: Kadra zarządzająca oraz pracownicy administracyjni i techniczni.
2.4. Maksymalna liczba uczestników w jednej grupie: 25 osób.
3. Forma szkoleń:
3.1. Szkolenia stacjonarne w siedzibie Urzędu.
3.2. Metody szkoleniowe: wykłady, warsztaty, ćwiczenia praktyczne.
4. Czas trwania szkolenia pracowników dla jednej grupy: minimum 3 - 4 godziny.
5. Czas trwania szkolenia kadry zarządzającej minimum 2 godziny.
6. Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00- 15:00.
7. Materiały szkoleniowe:
7.1. Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
7.2. Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.
8. Wymagania dotyczące wykonawcy
8.1. Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z zakresu bezpieczeństwa informacji.
8.2. Preferowane certyfikaty i akredytacje trenerów.
8.3. Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.
9. Konspekt szkolenia:
9.1. Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
9.2. Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia

10. Ewaluacja szkoleń:
10.1. Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
10.2. Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
10.3. Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
10.4. Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
10.5. Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.