Załącznik nr 3 do Warunków zamówienia /WZ/

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest przeprowadzenie szkoleń podstawowych i specjalistycznych dla pracowników Starostwa Powiatowego we Włocławku oraz przeprowadzenie audytu cyberbezpieczeństwa w ramach projektu grantowego „Cyberbezpieczny Samorząd”.

Zadanie jest dofinansowane przez Unię Europejską w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) „Cyberbezpieczny samorząd”; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0948/FERC.02.02-CS.01-001/23/2024.

1. **Ogólny opis przedmiotu zamówienia.**

Wszystkie oferowane szkolenia muszą pochodzić z legalnego kanału sprzedaży producenta i odbywać się w języku polskim oraz na terytorium Polski.

Szkolenia muszą być przeprowadzone w terminach uzgodnionych z Zamawiającym  
i odbywać się wyłącznie w dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, a w danym terminie może odbywać się tylko jedno ze wskazanych dalej szkoleń. Wykonawca w ramach realizacji przedmiotu zamówienia przygotuje harmonogram oraz program szkoleń i dostarczy go do akceptacji przez Zamawiającego, w terminie nie późniejszym niż 5 dni roboczych przed początkiem terminu szkoleń.

Wykonawca zapewni:

* materiały dydaktyczne dla uczestników szkolenia, odzwierciedlające całość omawianych zagadnień, w tym dostęp do certyfikowanych materiałów szkoleniowych;
* wykładowcę/wykładowców posiadającego/posiadających odpowiednie kwalifikacje zawodowe.

a dodatkowo, w przypadku szkoleń wymienionych w punkcie II.1:

* salę szkoleniową oraz sprzęt niezbędny do przeprowadzenia szkolenia;
* zakwaterowanie i nocleg w miejscowości szkolenia wraz z pełnym wyżywieniem (śniadanie, obiad, kolacja).

Wykonawca zrealizuje usługę szkoleniową zgodnie z dalej podanym opisem i dla dalej wskazanej liczby uczestników.

1. **Szczegółowy podział przedmiotu zamówienia.**
2. Szkolenie dla pracowników Starostwa Powiatowego we Włocławku, zatrudnionych na stanowisku Starszy Informatyk, Informatyk na temat:

a) Administrowanie systemem Windows Server MS – 55344

b) Instalacja, przechowywanie i obliczenia z systemem Windows Server MS - 55341

c) Migracja w centrum danych Windows Server

d) Konfiguracja, zarządzanie i odzyskiwanie - Veeam Backup.

1. Szkolenie dla pracowników Starostwa Powiatowego we Włocławku, zatrudnionych na stanowisku Starszy Informatyk, Informatyk na temat: IT NETGEAR.
2. Szkolenie dla pracowników Starostwa Powiatowego we Włocławku na temat cyberbezpieczeństwa na stanowisku pracy urzędnika samorządowego.
3. Audyt cyberbezpieczeństwa w Starostwie Powiatowym we Włocławku.

***Szkolenia specjalistyczne dla pracowników Starostwa Powiatowego we Włocławku***

1. **Szczegółowy opis podzielonych części przedmiotu zamówienia.**

**III.1.a) Szkolenie dla pracowników Starostwa Powiatowego we Włocławku zatrudnionych na stanowisku Starszy Informatyk, Informatyk - na temat: Administrowanie systemem Windows Server MS – 55344**

1. **Forma szkolenia:** Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego lub w miejscu wskazanym przez Wykonawcę (jeżeli szkolenia będą realizowane poza siedzibą Zamawiającego, Wykonawca musi zapewnić nocleg z wyżywieniem w miejscowości, w której będzie prowadzone szkolenie na czas jego trwania).
2. **Liczba uczestników szkolenia:** 2 osoby.
3. **Czas trwania szkolenia:**

Liczba dni: minimum 5 dni;

Liczba godzin: minimum 40 godzin lekcyjnych; w tym, minimum 15 godzin laboratoriów (zajęć praktycznych).

1. **Zakres merytoryczny szkolenia:**
   1. **Wprowadzenie do administracji systemu Windows Server**

* Wprowadzenie do systemu Windows Server
* Wprowadzenie do systemu Windows Server Core
* Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server

Ćwiczenie: Wdrażanie i konfiguracja systemu Windows Server

* Wdrażanie i konfiguracja systemu Server Core
* Wdrażanie i stosowanie zdalnej administracji serwerami
  1. **Usługi zarządzania tożsamością w systemie Windows Server**
* Wprowadzenie do AD DS
* Wdrażanie kontrolerów domeny Windows Server
* Wprowadzenie do usługi Azure AD
* Wdrażanie zasad grupy
* Wprowadzenie do usług certyfikatów Active Directory

Ćwiczenie: Wdrażanie usług zarządzania tożsamością i zasad grupy

* Wdrażanie nowego kontrolera domeny w systemie Server Core
* Konfigurowanie zasad grupy
* Wdrażanie i korzystanie z usług certyfikatów
* Wyjaśnienie podstaw zasad grupy i konfiguracja GPO w środowisku domenowym
* Opis roli usług certyfikatów Active Directory i korzystanie z certyfikatów
  1. **Usługi infrastruktury sieciowej w systemie Windows Server**
* Wdrażanie i zarządzanie protokołem DHCP
* Wdrażanie i zarządzanie systemem DNS
* Wdrażanie i zarządzanie systemem IPAM
* Usługi dostępu zdalnego w systemie Windows Server

Ćwiczenie: Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server

* Wdrażanie i konfiguracja protokołu DHCP
* Wdrażanie i konfiguracja systemu DNS
* Wdrażanie serwera proxy aplikacji sieci WWW
  1. **Serwery plików i zarządzanie pamięcią masową w systemie Windows Server**
* Woluminy i systemy plików w systemie Windows Server
* Wdrażanie udostępniania w systemie Windows Server
* Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
* Wdrażanie deduplikacji danych
* Wdrażanie interfejsu iSCSI
* Wdrażanie rozproszonego systemu plików

Ćwiczenie: Wdrażanie rozwiązań pamięci masowej w systemie Windows Server

* Wdrażanie deduplikacji danych
* Konfiguracja magazynu iSCSI
* Konfiguracja nadmiarowych przestrzeni dyskowych
* Wdrażanie Storage Spaces Direct
  1. **Wirtualizacja Hyper-V i kontenery w systemie Windows Server**
* Hyper-V w systemie Windows Server
* Konfiguracja maszyn wirtualnych /li>
* Zabezpieczanie wirtualizacji w systemie Windows Server
* Kontenery w systemie Windows Server
* Wprowadzenie do platformy Kubernetes

Ćwiczenie: Wdrażanie i konfiguracja wirtualizacji w systemie Windows Server

* Tworzenie i konfigurowanie maszyn wirtualnych
* Instalacja i konfiguracja kontenerów
  1. **Wysoka dostępność w systemie Windows Server**
* Planowanie wdrożenia klastra pracy awaryjnej
* Tworzenie i konfiguracja klastra pracy awaryjnej
* Wprowadzenie do rozciągniętych klastrów
* Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V

Ćwiczenie: Wdrażanie klastra pracy awaryjnej

* Konfiguracja pamięci masowej i tworzenie klastra
* Wdrażanie i konfiguracja serwera plików o wysokiej dostępności
* Sprawdzanie poprawności wdrożenia serwera plików o wysokiej dostępności
  1. **Odzyskiwanie danych po awarii w systemie Windows Server**
* Funkcja Hyper-V Replica
* Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server

Ćwiczenie: Wdrażanie funkcji Hyper-V Replica i Windows Server Backup

* Wdrażanie funkcji Hyper-V Replica
* Wdrażanie tworzenia kopii zapasowych i przywracania za pomocą narzędzia Windows Server Backup
  1. **Bezpieczeństwo systemu Windows Server**
* Ochrona danych uwierzytelniających i dostępu uprzywilejowanego
* Hardening systemu Windows Server
* JEA w systemie Windows Server
* Zabezpieczanie i analiza ruchu w SMB
* Zarządzanie aktualizacjami w systemie Windows Server

Ćwiczenie: Konfiguracja zabezpieczeń w systemie Windows Server

* Konfiguracja funkcji Windows Defender Credential Guard
* Lokalizowanie problematycznych kont
* Wdrażanie rozwiązania LAPS
  1. **RDS (usługi pulpitu zdalnego) w systemie Windows Server**
* Wprowadzenie do RDS
* Konfiguracja wdrażania pulpitu opartego na sesji
* Wprowadzenie do osobistych i połączonych pulpitów wirtualnych

Ćwiczenie: Wdrażanie RDS w systemie Windows Server

* Wdrażanie RDS
* Konfigurowanie ustawień kolekcji sesji i wykorzystywanie RDC
* Konfiguracja szablonu pulpitu wirtualnego.
  1. **Dostęp zdalny i usługi internetowe w systemie Windows Server**
* Wdrażanie sieci VPN
* Wdrażanie usługi Always On VPN
* Wdrażanie systemu NPS
* Wdrażanie serwera WWW w systemie Windows Server

Ćwiczenie: Wdrażanie obciążeń sieciowych

* Wdrażanie sieci VPN w systemie Windows Server
* Wdrażanie i konfiguracja serwera WWW
  1. **Monitorowanie serwera i wydajności w systemie Windows Server**
* Wprowadzenie do narzędzi do monitorowania systemu Windows Server
* Korzystanie z monitora wydajności
* Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów

Ćwiczenie: Monitorowanie i rozwiązywanie problemów z systemem Windows Server

* Ustanowienie bazowego poziomu wydajności
* Identyfikacja źródła problemu z wydajnością.
  1. **Aktualizacja i migracja w systemie Windows Server**
* Migracja AD DS
* Usługa migracji pamięci masowej
* Narzędzia do migracji systemu Windows Server

Ćwiczenie: Migracja obciążeń serwera

* Wdrażanie usługi migracji pamięci masowej

1. **Trener realizujący szkolenie.**

Trener, skierowany do realizacji usługi szkoleniowej, musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

1. **Certyfikat ukończenia szkolenia:**

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkoleniasygnowany przez Producenta oprogramowania Zamawiającego.

**III.1.b) Szkolenie dla pracowników Starostwa Powiatowego we Włocławku zatrudnionych na stanowisku Starszy Informatyk, Informatyk - na temat: Instalacja, przechowywanie i obliczenia z systemem Windows Server MS – 55341**

1. **Forma szkolenia:** Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego lub w miejscu wskazanym przez Wykonawcę (jeżeli szkolenia będą realizowane poza siedzibą Zamawiającego, Wykonawca musi zapewnić nocleg z wyżywieniem w miejscowości, w której będzie prowadzone szkolenie na czas jego trwania).
2. **Liczba uczestników szkolenia:** 2 osoby.
3. **Czas trwania szkolenia:** liczba dni - minimum 4 dni.
4. **Zakres merytoryczny szkolenia:**
   1. **Instalacja, aktualizacja i migracja serwerów i obciążeń**

Ćwiczenie:

* systemu Windows Server Datacenter.
* Instalacja Konfiguracja systemu Windows Server z tworzeniem adresów IP.
* Weryfikacja i włączenie roli serwera WWW w systemie Windows Server.
* Migracja i weryfikacja roli DHCP.
* Instalacja, aktualizacja i migracja serwerów i obciążeń
  1. **Konfiguracja lokalnej pamięci masowej**

Ćwiczenie:

* Konfiguracja dysku z MBR i GBT.
* Konfigurowanie dysków dynamicznych z MBR i GPT
* Tworzenie woluminu, formatowanie i przypisywanie dysku.
* Użyj zarządzania dyskami, aby przekonwertować dysk dynamiczny na dysk podstawowy.
* Tworzenie i dołączanie wirtualnego dysku twardego.
  1. **U Implementacja przestrzeni dyskowych i deduplikacji danych**

Ćwiczenie:

* Zainstaluj File Server i iSCSI Target Server na Windows Server.
* Utwórz nowy obiekt docelowy iSCSI z nowym dyskiem.
* Skonfiguruj połączenia sieciowe.
* Konfiguracja wielościeżkowego wejścia/wyjścia (MPIO).
* Konfiguracja inicjatora iSCSI.
* Tworzenie udziałów.
  1. **Implementacja przestrzeni dyskowych i deduplikacji danych Instalacja i konfiguracja Hyper-V i maszyn wirtualnych**

Ćwiczenie:

* Tworzenie puli pamięci masowej
* Tworzenie dysku lustrzanego
* Tworzenie woluminów na dyskach wirtualnych
* Instalowanie roli deduplikacji danych
* Włączanie deduplikacji danych na woluminach
  1. **Instalacja i konfiguracja Hyper-V i maszyn wirtualnych**

Ćwiczenie:

* Weryfikacja ustawień i konfiguracji sieci.
* Tworzenie prywatnych i wewnętrznych przełączników wirtualnych.
* Tworzenie maszyn wirtualnych.
* Weryfikacja konfiguracji sieci na maszynach wirtualnych.
* Zarządzanie punktami kontrolnymi.
* Włączanie serwera repliki.
  1. **Wysoka dostępność w systemie Windows Wdrażanie i zarządzanie kontenerami Windows i Hyper-V**

Ćwiczenie:

* Zainstaluj funkcję kontenerów za pomocą Menedżera serwera.
* Włącz konfigurację sieci.
* Instalacja pakietu Docker
* Pobranie obrazu Docker systemu Windows Server
* Instalacja Centrum administracyjnego Windows
  1. **Wdrożenie klastra pracy awaryjnej**

Ćwiczenie:

* Utwórz serwer docelowy iSCI.
* Podłączenie klastra do współdzielonej pamięci masowej.
* Zainstaluj i zweryfikuj funkcję klastra pracy awaryjnej systemu Windows Server.
* Utwórz klaster pracy awaryjnej.
* Konfigurowanie ustawień przełączania awaryjnego i przywracania awaryjnego.
  1. **Implementacja klastra pracy awaryjnej z Windows Server Hyper-V**

Ćwiczenie:

* Podłącz węzły klastra do pamięci masowej.
* Zainstaluj Hyper-V na węzłach.
* Zainstalowanie funkcji klastra pracy awaryjnej i utworzenie klastra Hyper-V.
* Utwórz wolumin udostępniony klastra
* Utwórz wysoce dostępną maszynę wirtualną.
* Przeprowadzenie przełączania awaryjnego.
  1. **RDS (usługi pulpitu zdalnego) w systemie Window Zarządzanie, monitorowanie i utrzymywanie instalacji maszyn wirtualnych**

Ćwiczenie:

* Symulacja awarii serwera.
* Funkcjonalność obserwowania zdarzeń.
* Obsługa dzienników usługi katalogowej i serwera DNS.
* Konfiguracja subskrypcji dziennika zdarzeń i dzienników zabezpieczeń.
* Zastosowanie konfiguracji PowerShell Desired State

1. **Trener realizujący szkolenie.**

Trener, skierowany do realizacji usługi szkoleniowej, musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

1. **Certyfikat ukończenia szkolenia.**

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkoleniasygnowany przez Producenta oprogramowania Zamawiającego.

**III.1.c) Szkolenie dla pracowników Starostwa Powiatowego we Włocławku zatrudnionych na stanowisku Starszy Informatyk, Informatyk - na temat: Migracja w centrum danych Windows Server.**

* 1. **Forma szkolenia:** Szkolenie realizowane w formie stacjonarnej, w siedzibie Zamawiającego lub w miejscu wskazanym przez Wykonawcę (jeżeli szkolenia będą realizowane poza siedzibą Zamawiającego, Wykonawca musi zapewnić nocleg z wyżywieniem w miejscowości, w której będzie prowadzone szkolenie na czas jego trwania).
  2. **Liczba uczestników:** 2 osoby.
  3. **Czas trwania szkolenia:**

Liczba dni: minimum 2 dni;

Liczba godzin: minimum 16 godzin lekcyjnych.

* 1. **Zakres merytoryczny szkolenia.**

**3.1. Strategia centrum danych**

**3.2. Zarządzanie projektami**

**3.3. Zarządzanie ryzykiem**

**3.4. Strategie migracyjne**

**3.5. Aspekty prawne**

**3.6. Projektowanie docelowego centrum danych**

**3.7. Bezpieczeństwo centrum danych**

**3.8. Zarządzanie bezpieczeństwem podczas migracji**

* 1. **Trener realizujący szkolenie.**

Trener, skierowany do realizacji usługi szkoleniowej, musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

* 1. **Certyfikat ukończenia szkolenia.**

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkoleniasygnowany przez Producenta oprogramowania Zamawiającego.

**III.1.d) Szkolenie dla pracowników Starostwa Powiatowego we Włocławku zatrudnionych na stanowisku Starszy Informatyk, Informatyk - na temat: Konfiguracja, zarządzanie i odzyskiwanie - Veeam Backup**

1. **Forma szkolenia:** szkolenie realizowane online.
2. **Liczba uczestników:** 2 osoby
3. **Czas trwania szkolenia**:

Liczba dni: minimum 4 dni.

Liczba godzin: minimum 32 godziny lekcyjne.

1. **Zakres merytoryczny szkolenia.**

**4.1. Strategie ochrony danych**

**4.2. Analiza ryzyka dla danych**

**4.3. Co jest chronione ?**

**4.4. Kwestie bezpieczeństwa i ochrony**

**4.5 Ochrona obciążeń**

**4.6. Nieustrukturyzowana kopia zapasowa danych**

**4.7. Optymalizacja kopii zapasowych**

**4.8. Zmienność i utwardzone repozytoria**

**4.9. Optymalizacja infrastruktury kopii zapasowych**

**4.10. Replikacja**

**4.11. Zadania dotyczące kopii zapasowych**

**4.12. Długoterminowa retencja**

**4.13. Scale-out Backup RepositoryTM**

**4.14. Przenoszenie i kopiowanie kopii zapasowych za pomocą VeeaMover**

**4.15. Weryfikacja odzyskiwania**

**4.16. Veeam Backup Enterprise Manager**

**4.17. Planowanie reakcji na incydent**

**4.18. Zaawansowane funkcje odzyskiwania**

**4.19. Wybór idealnej metody odzyskiwania**

**4.20. Ustalenie właściwej ścieżki odzyskiwania**

**4.21 Laboratorium 1: Bezpieczny serwer kopii zapasowych Veeam**

**4.22. Laboratorium 2: Ochrona maszyny wirtualne**

**4.23. Laboratorium 3: Veeam Agent funkcje tworzenia kopii zapasowych**

**4.24. Laboratorium 4: Nieustrukturyzowane funkcje tworzenia kopii zapasowych danych**

**4.25. Laboratorium 5: Optymalizacja infrastruktury zapasowej**

**4.26. Laboratorium 6: Drugie tworzenie kopii zapasowych i backupu witryny**

**4.27. Laboratorium 7: Budowanie zdolności replikacji**

**4.28. Laboratorium 8: Testowanie kopii zapasowych maszyn wirtualnych**

**4.29. Laboratorium 9: Współpraca z Veeam Backup Enterprise Manager**

**4.30. Laboratorium 10: Odzyskiwanie elementów aplikacji**

**4.31. Laboratorium 11: Odzyskiwanie pliku z systemem operacyjnym gościa**

**4.32. Laboratorium 12: Odzyskiwanie maszyn wirtualnych**

**4.33. Laboratorium 13: Przywracanie fizycznej maszyny z kopii zapasowej agenta**

**4.34. Laboratorium 14: Przywracanie z repliki**

**4.35. Laboratorium 15: Przywracanie z kopii zapasowej**

1. **Trener realizujący szkolenie.**

Trener, skierowany do realizacji usługi szkoleniowej, musi posiadać certyfikat wystawiony przez Producenta oprogramowania.

1. **Certyfikat ukończenia szkolenia.**

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkoleniasygnowany przez Producenta oprogramowania Zamawiającego.

**III.2. Szkolenie dla pracowników Starostwa Powiatowego we Włocławku zatrudnionych na stanowisku Starszy Informatyk, Informatyk - na temat: IT NETGEAR.**

1. **Forma szkolenia:** Szkolenie realizowane stacjonarnie w siedzibie Zamawiającego oraz w części w formie online.
2. **Liczba uczestników szkolenia:** 2 osoby.
3. **Czas trwania szkolenia.**

Liczba dni: 3 dni.

Liczba godzin: minimum 12 godzin (minimum 4 godziny każdego dnia w siedzibie Zamawiającego oraz 4 godziny online).

1. **Zakres merytoryczny szkolenia.**
   1. **Gwarancja, rejestracja, support techniczny, upgrad FW**
   2. **Konfiguracji przełączników z pomocą CLI, WWW oraz Engage,**
   3. **Presety AV, Vlany, DHCP**
   4. **Topologie sieci**
   5. **Konfiguracja stosu**
   6. **Różnice w konfiguracji dla topologii łańcuch, gwiazda, pierścień z możliwością komunikacji z siecią zewnętrzną / klienta, ruting statyczny**
   7. **Konfiguracja przełączników typu Core z wykorzystaniem LAG i weryfikacja zajętości uplink’ów miedzianych oraz światłowodowych,**
   8. **IGMP, STP jak NETGEAR podszedł do tych zagadnień.**
   9. **Diagnostyka**
   10. **Wymiana danych z przełącznikami L3 innych serii (nie AV), producentów np. Netgear, Cisco, tplink itp.**
   11. **802.1x**
2. **Certyfikat ukończenia szkolenia.**

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkoleniasygnowany przez Producenta sprzętu sieciowego Zamawiającego.

***Szkolenia podstawowe dla pracowników Starostwa Powiatowego we Włocławku***

**III.3. Szkolenie dla pracowników Starostwa Powiatowego we Włocławku na temat cyberbezpieczeństwa na stanowisku pracy urzędnika samorządowego.**

1. **Forma szkolenia:** Szkolenie realizowane w formie stacjonarnej w siedzibie Zamawiającego.
2. **Liczba uczestników:** 130 osób (podzielone na 4 grupy – każda grupa inny termin szkolenia).
3. **Czas trwania szkolenia –** 4 godziny lekcyjne
4. **Zakres merytoryczny szkolenia.**

**4.1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika. Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.**

**4.2. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony Www, ataki przez telefon, ataki przez komunikatory i social media, phishing, spoofing, spam itp.**

**4.3. Wykorzystywanie nieładu informacyjnego (dezinformacji, deep fake, fake news itp.). Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko".**

**4.4. Bezpieczna praca z urządzeniami mobilnymi oraz przechowywanie danych, bezpieczeństwo poczty e-mail, przechowywanie danych w chmurze.**

**4.5. Prawidłowe korzystanie z oprogramowania antywirusowego.**

**4.6. Zasady aktualizacji programów i aplikacji.**

**4.7. Szyfrowanie dokumentów i poczty elektronicznej.**

**4.8. Polityka haseł, zarządzanie dostępem i tożsamością.**

**4.9. Zasady bezpiecznej pracy zdalnej.**

**4.10. Korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym zagrożenia. Zdalny dostęp do zasobów jednostki - bezpieczna praca  
z plikami.**

**4.11. Zasady komunikacji w trybie pracy zdalnej.**

**3.12. Zalecenia PUODO dla pracodawcy i pracownika podczas pracy zdalnej.**

1. **Trener realizujący szkolenie.**

Trener musi posiadać certyfikat audytora wiodącego ISO-27001.

1. **Certyfikat ukończenia szkolenia.**

Po ukończeniu szkolenia, uczestnicy szkolenia muszą otrzymać certyfikat ukończenia szkolenia.

***Audyt Cyberbezpieczeństwa***

**III.4. Audyt cyberbezpieczeństwa w Starostwie Powiatowym we Włocławku.**

1. **Zakres usługi:**
   1. **Analiza wstępna stanu bezpieczeństwa informacji w starostwie w zakresie objętym Audytem.**
   2. **Zebranie wstępnych odpowiedzi i dowodów audytowych.**
   3. **Wspólne zdefiniowanie rekomendowanych działań korygujących w zakresie objętym Audytem w oparciu o poniższe założenia:**

**1.3a) Audyt Początkowy:**

* + Przegląd polityk bezpieczeństwa informacji (SZBI).
  + Ocena mechanizmów zarządzania ryzykiem cyberbezpieczeństwa.
  + Testy penetracyjne i analiza podatności systemów IT.
  + Przegląd procedur reagowania na incydenty.

**1.3b) Audyt Końcowy:**

* + Ponowna ocena polityk bezpieczeństwa informacji (SZBI).
  + Sprawdzenie wdrożonych mechanizmów zarządzania ryzykiem.
  + Powtórne testy penetracyjne i analiza podatności.
  + Przegląd procedur reagowania na incydenty po implementacji rekomendacji.
  1. **Wykonanie audytu zgodnie z wymaganiami ustawy z dnia 5 lipca 2018 r.  
     o Krajowym Systemie Cyberbezpieczeństwa** **(Dz.U. z 2024 r. poz. 1077 ze zm.) oraz rozporządzenia 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. z 2024 r. poz. 773 ze zm.).**
  2. **Przeprowadzenie testów bezpieczeństwa w zakresie:**

**1.5a)** stron dostępnych pod adresami:

<https://www.wloclawski.pl> oraz <https://bip.wloclawski.pl/>

**1.5b)** styku sieci urzędu z Internetem

**1.5c)** serwerów i urządzeń sieciowych

**1.5d)** wykonanie raportu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących

* 1. **Wykonanie serii testów phishingowych dla 120 pracowników urzędu.**
  2. **Analiza ostateczna po wdrożeniu rozwiązań poprawiających cyberbezpieczeństwo wykonana przez certyfikowanego audytora (Audyt zgodny z ustawą o KSC)**
  3. **Wywiady audytowe oraz zebranie dowodów.**
  4. **Aktualizacja dokumentacji SZBI Starostwa w oparciu o poniższe kryteria:**

**Weryfikacja istniejącej dokumentacji SZBI:**

**1.9a) Zakres weryfikacji:**

* + - Analiza zgodności z normami ISO/IEC 27001 oraz przepisami KRI i RODO.
    - Ocena skuteczności wdrożonych procedur i polityk.
    - Identyfikacja braków i obszarów do poprawy.

**1.9b) Kroki weryfikacji:**

* + - Przegląd i aktualizacja dokumentacji.
    - Konsultacje z kluczowym personelem.
    - Testowanie efektywności wdrożonych procedur.
    - Raportowanie wyników weryfikacji i proponowanie usprawnień.

**1.9c) Zakres dokumentacji:**

* + - Polityka bezpieczeństwa informacji.
    - Procedury operacyjne dotyczące zarządzania bezpieczeństwem.
    - Instrukcje dotyczące reagowania na incydenty.
    - Plany awaryjne i zarządzania kryzysowego.

**1.9d) Kroki wdrożenia:**

* + - Identyfikacja i analiza wymagań prawnych i regulacyjnych.
    - Opracowanie polityk i procedur.
    - Szkolenia dla pracowników w zakresie nowo utworzonych dokumentów.
    - Implementacja i monitorowanie przestrzegania nowych polityk.

1. Wykonawca musi posiadać certyfikat normy ISO-27001 oraz normy ISO-9001