



## **OPIS PRZEDMIOTU ZAMÓWIENIA (CZĘŚĆ KOMPETECYJNA)**

**„Przeprowadzenie szkolenia dla personelu IT”, w ramach projektu „Poprawa cyberbezpieczeństwa informacji w Gminie Chorkówka.” - Obszar 3 Kompetencyjny na podstawie konkursu grantowego w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23 Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027**

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

80500000-9	Usługi szkoleniowe
80510000-2	Usługi szkolenia specjalistycznego
72222300-0	Usługi w zakresie technologii informacji
80330000-6	Usługi edukacji w zakresie bezpieczeństwa



## Cyberbezpieczny Samorząd

### 1. Wymagania

Oferty na szkolenia dla personelu IT muszą obejmować przeszkolenie 2 pracowników Zamawiającego.

Czas realizacji szkoleń: do dnia 30.04.2026 r.

Czas wykonania szkoleń zostanie określony w formie harmonogramu sporządzonego po podpisaniu umowy. Harmonogram ten wymaga akceptacji Zamawiającego. Zamawiający może w terminie 3 dni roboczych wnieść uwagi i zastrzeżenia do harmonogramu które wykonawca zobowiązany jest uwzględnić. Brak wniesienia uwag w powyższym terminie oznacza akceptację harmonogramu przez Zamawiającego.

Szkolenia mogą odbyć się na zasadzie dostarczenia przez oferenta VOUCHERA na dane szkolenie, uprawniającego do odbycia szkolenia przez pracownika.

Materiały szkoleniowe udostępnione w wersji elektronicznej muszą spełniać standardy dostępności cyfrowej oraz przeciwdziałania stereotypom tj. ew. wizualizacje będą uwzględniały w szczególności rodzaj męski (np. na mat. zdjęciowych czy grafikach z udziałem ludzi, zawsze będzie również postać męska)

### 2. Zakres przedmiotu zamówienia

#### a) Zarządzanie usługą Active Directory w środowisku Windows Server 2023

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Gminy
Zakres szkolenia	<u>Instalacja i konfiguracja kontrolerów domeny</u> <ol style="list-style-type: none"><li>1. Omówienie usług AD DS</li><li>2. Omówienie kontrolerów domeny usług AD DS</li><li>3. Wdrożenie kontrolera domeny</li><li>4. Encrypted DNS - szyfrowana usługa rozpoznawania nazw w Windows Server 2022</li></ol> <u>Zarządzanie obiektami w AD DS</u> <ol style="list-style-type: none"><li>1. Zarządzanie kontami użytkowników</li><li>2. Zarządzanie grupami w usługach AD DS</li><li>3. Zarządzanie obiektami typu komputer w AD DS</li><li>4. Wdrażanie i zarządzanie OU</li></ol> <u>Zarządzanie zaawansowaną infrastrukturą AD DS</u> <ol style="list-style-type: none"><li>1. Wprowadzenie do zaawansowanych wdrożeń AD DS</li></ol>

str. 2



## Cyberbezpieczny Samorząd

	<ul style="list-style-type: none"><li>2. Wdrożenie rozproszonego środowiska AD DS</li><li>3. Konfiguracja relacji zaufania AD DS</li></ul> <p><u>Wdrażanie i zarządzanie lokacjami i repliką AD DS</u></p> <ul style="list-style-type: none"><li>1. Omówienie replikacji usług AD DS</li><li>2. Konfigurowanie lokacji usług AD DS</li></ul> <p>Konfigurowanie i monitorowanie replikacji usług AD DS.</p> <p><u>Wdrażanie zasad grupy</u></p> <ul style="list-style-type: none"><li>1. Wprowadzenie do zasad grupy</li><li>2. Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)</li><li>3. Konfiguracja zakresu i przetwarzania obiektów GPO</li><li>4. Rozwiązywanie problemów z GPO</li></ul> <p><u>Zarządzanie ustawieniami użytkowników za pomocą zasad grupy</u></p> <ul style="list-style-type: none"><li>1. Wdrażanie szablonów administracyjnych</li><li>2. Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów</li><li>3. Konfiguracja preferencji zasad grupowych</li></ul>
Typ szkolenia	Szkolenie On-line w języku Polskim
Liczba uczestników	2 osoba
Czas trwania	Minimum 2 dni (16 godzin)
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Kontakt z trenerem po szkoleniu	14 dni

### b) ESET Inspect - Administrator XDR

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Gminy



## Cyberbezpieczny Samorząd

Zakres szkolenia	1. Omówienie pojęcia Extended Detection & Respond (XDR), 2. Architektura produktu ESET Inspect, 3. Wdrożenie serwera ESET Inspect (ćwiczenie), 4. Wdrożenie i konfiguracja agentów ESET Inspect (ćwiczenie), 5. Omówienie funkcji ESET Inspect, 6. Generowanie detekcji i ich analiza (ćwiczenie), 7. Reguły i automatyzacja (ćwiczenie), 8. Raportowanie, powiadomienia i zarządzanie uprawnieniami, 9. Rozwiązywanie problemów.
Typ szkolenia	On-line w języku Polskim
Liczba uczestników	2 osoba
Czas trwania	Minimum 1 dni (7 godzin)
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Kontakt z trenerem po szkoleniu	14 dni

### c) CCNA Cisco Certified Network Associate

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Gminy



## Cyberbezpieczny Samorząd

Zakres szkolenia	<p><u>Wprowadzenie do sieci komputerowych i systemu Cisco IOS</u></p> <ol style="list-style-type: none"><li>1. Wprowadzenie do sieci komputerowych</li><li>2. Wprowadzenie do systemu Cisco IOS - podstawy pracy na przełączniku i routerze</li><li>3. Model sieciowy ISO/OSI, Model sieciowy TCP/IP. Omówienie i porównanie poszczególnych warstw</li><li>4. Adresacja IPv4, podział na podsieci</li><li>5. Podstawy protokołu IPv6</li></ol> <p><u>Praca w sieciach lokalnych</u></p> <ol style="list-style-type: none"><li>1. Działanie przełączanej sieci lokalnej: działanie przełącznika, ARP, brama domyślna</li><li>2. Konfiguracja i podstawowe zabezpieczenie przełącznika</li><li>3. VLANY oraz routing pomiędzy VLAN'ami</li><li>4. Diagnostowanie i rozwiązywanie problemów w sieciach lokalnych</li></ol> <p><u>Routing oraz protokoły routingu dynamicznego</u></p> <ol style="list-style-type: none"><li>1. Poznanie funkcji routing</li><li>2. Routing statyczny i dynamiczny</li><li>3. Wprowadzenie do protokołu routingu jednoobszarowego OSPF</li></ol> <p><u>Redundancja w sieciach</u></p> <ol style="list-style-type: none"><li>1. Budowanie redundantnych przełączanych topologii, protokół STP</li><li>2. Agregacja portów (EtherChannel)</li><li>3. Redundancja bramy domyślnej (HSRP)</li></ol> <p><u>Wybrane funkcje realizowane na urządzeniach Cisco</u></p> <ol style="list-style-type: none"><li>1. Listy dostępu ACL</li><li>2. DHCP i NAT na routerach Cisco</li><li>3. Sieci bezprzewodowe</li><li>4. Podstawy zarządzania obrazami Cisco IOS</li><li>5. Wprowadzenie do jakości usług QoS</li></ol> <p><u>Teoretyczne omówienie wybranych technologii sieciowych</u></p>
------------------	---



## Cyberbezpieczny Samorząd

	<ol style="list-style-type: none"><li>1. Wprowadzenie do wirtualizacji</li><li>2. Wprowadzenie do ewolucji sieci inteligentnych</li><li>3. Konfiguracja podstawowych narzędzi do monitorowania systemu IOS</li><li>4. Podstawowe aspekty zabezpieczenia sieci komputerowych</li><li>5. Technologie sieci WAN</li></ol>
Typ szkolenia	On-line w języku Polskim
Liczba uczestników	2 osoba
Czas trwania	Minimum 5 dni (35 godzin)
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Kontakt z trenerem po szkoleniu	14 dni

### d) Wirtualizacja Hyper-V, magazynowanie i przetwarzanie danych w środowisku Microsoft Windows Server

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny
Jednostka organizacyjna	Urząd Gminy



Zakres szkolenia	<p><u>Omówienie funkcji administracyjnych systemu Windows Server</u></p> <ol style="list-style-type: none"><li>1. Informacje wstępne o systemie Windows Server</li><li>2. Omówienie najważniejszych funkcji systemu Windows Server</li><li>3. Omówienie zasad i narzędzi związanych z zarządzaniem systemem Windows Server</li></ol> <p><u>Zarządzanie serwerami plików i pamięcią masową w systemie Windows Server</u></p> <ol style="list-style-type: none"><li>1. Wolumeny i systemy plików w systemie Windows Server</li><li>2. Współużytkowanie zasobów w systemie Windows Server</li><li>3. Wdrażanie obszarów pamięci masowej w systemie Windows Server</li><li>4. Wdrażanie funkcji deduplikacji danych</li><li>5. Wdrażanie protokołu iSCSI</li><li>6. Wdrażanie rozproszonego systemu plików</li><li>7. Migracja magazynu danych w Windows Server 2022</li></ol> <p><u>Oprogramowanie do wirtualizacji Hyper-V i kontenery w systemie Windows Server</u></p> <ol style="list-style-type: none"><li>1. Hyper-V w systemie Windows Server</li><li>2. Konfigurowanie maszyn wirtualnych</li><li>3. Zabezpieczenie wirtualizacji w systemie Windows Server</li><li>4. Ulepszenia działania wirtualnego przełącznika sieciowego w Windows Server 2022</li><li>5. Kontenery w systemie Windows Server</li></ol> <p><u>Funkcje wysokiej dostępności w systemie Windows Server</u></p> <ol style="list-style-type: none"><li>1. Planowanie wdrażania klastrów na potrzeby przełączania awaryjnego</li><li>2. Tworzenie i konfigurowanie klastra przełączania awaryjnego</li><li>3. Omówienie klastrów rozległych</li><li>4. Funkcje wysokiej dostępności i rozwiązania do usuwania skutków awarii oparte na maszynach wirtualnych Hyper-V</li></ol> <p><u>Usuwanie skutków awarii w systemie Windows Server</u></p> <ol style="list-style-type: none"><li>1. Funkcja Hyper-V Replica</li><li>2. Infrastruktura tworzenia i odtwarzania kopii zapasowych w systemie</li></ol>
------------------	--



## Cyberbezpieczny Samorząd

	<p>Windows Server</p> <p><u>Implementowanie i zarządzanie zasobami typu failover clustering</u></p> <ol style="list-style-type: none"> <li>1. Planowanie strategii wdrożenia typu failover cluster</li> <li>2. Tworzenie i konfiguracja struktury failover cluster</li> <li>3. Monitoring infrastruktury</li> </ol> <p><u>Implementowanie rozwiązań typu failover clustering dla maszyn wirtualnych w Hyper-V</u></p> <ol style="list-style-type: none"> <li>1. Prezentacja i integracja Hyper-V w Windows Server 2016 wraz z failover clustering</li> <li>2. Implementacja i zarządzanie maszynami wirtualnymi w Hyper-V w failover clusters</li> <li>3. Główne cechy wdrożeń maszyn wirtualnych w środowisku typu wysokiej dostępności i niezawodności</li> <li>4. Szyfrowane Cluster Shared Volumes w Windows Server 2022</li> </ol> <p><u>Implementowanie network load balancing</u></p> <ol style="list-style-type: none"> <li>1. Przegląd metod zastosowania klastrów typu NLB</li> <li>2. Konfiguracja klastrów NLB</li> <li>3. Planowanie i implementacja NLB</li> </ol>
Typ szkolenia	On-line w języku Polskim
Liczba uczestników	2 osoba
Czas trwania	Minimum 3 dni (24 godzin)
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Kontakt z trenerem po szkoleniu	14 dni

### e) Wdrażanie, zarządzanie i zabezpieczanie sieci za pomocą zasad grupy.

Atrybut	Wymagania minimalne, podstawowe, obligatoryjne, obowiązkowe
Obszar	Kompetencyjny





## Cyberbezpieczny Samorząd

Jednostka organizacyjna	Urząd Gminy
Zakres szkolenia	<p><u>Wprowadzenie do Group Policy</u></p> <ol style="list-style-type: none"><li>1. Group Policy i Active Directory</li><li>2. Przegląd Active Directory</li><li>3. Omówienie Group Policy</li></ol> <p><u>Narzędzia zarządzania Group Policy</u></p> <ol style="list-style-type: none"><li>1. wprowadzenie do Group Policy Management Console (GPMC)</li><li>2. instalacja GPMC</li><li>3. zaawansowane funkcje GPMC</li><li>4. funkcjonalności RSoP</li><li>5. filtry WMI</li></ol> <p><u>Projektowanie infrastruktury Group Policy</u></p> <ol style="list-style-type: none"><li>1. implementacja Group Policy</li><li>2. planowanie projektu Group Policy</li><li>3. projektowanie rozwiązań Group Policy</li><li>4. wdrażanie Group Policy</li><li>5. zarządzanie rozwiązaniami Group Policy</li></ol> <p><u>Rozwiązywanie problemów z Group Policy</u></p> <ol style="list-style-type: none"><li>1. infrastruktura Group Policy</li><li>2. kolejność wdrażania Group Policy</li><li>3. narzędzia rozwiązywania problemów z Group Policy</li></ol> <p><u>Wdrażanie szablonów zabezpieczeń</u></p> <ol style="list-style-type: none"><li>1. architektura zabezpieczeń</li><li>2. baza SECEDIT</li><li>3. zwiększanie zabezpieczeń kont komputerów</li></ol> <p><u>Wdrażanie zabezpieczeń za pomocą Group Policy</u></p> <ol style="list-style-type: none"><li>1. wprowadzenie do konfiguracji zabezpieczeń</li><li>2. zabezpieczenia domeny</li></ol>



3. kontrolowanie usług za pomocą Group Policy
4. wymuszanie polityk kontroli
5. ograniczanie członkostwa w grupach
6. wykorzystanie skryptów

### Konfiguracja środowiska stacji roboczych

1. skrypty klienckie
2. ustawienia pulpitu, Menu Start oraz paska zadań
3. ustawienia panelu sterowania
4. komponenty Windows
5. profile użytkowników
6. przekierowanie folderów
7. zarządzanie drukarkami
8. ustawienia sieci

### Przypisywanie i publikowanie pakietów aplikacji

1. paczki MSI
2. konfiguracja ustawień UV-E
3. metody wdrażania oprogramowania w GPO
4. wdrażanie oprogramowania
5. ustawienia punktów dystrybucji

### Systems Management Server

1. Polityki ograniczania oprogramowania (SRP)
2. przeznaczenie SRP
3. sposoby tworzenia polityk SRP
4. dodatkowe reguły
5. efektywne polityki SRP

### Tworzenie i wdrażanie szablonów administracyjnych (ADM)

1. wprowadzenie do ADM
2. standard szablonów ADM i ADMX
3. struktura rejestru i szablony ADM i ADMX
4. składnia szablonów ADM i ADMX



## Cyberbezpieczny Samorząd

	<p>5. dostosowywanie szablonów ADM i ADMX</p> <p><u>Nowe funkcje Group Policy w Windows 8.1 i Windows Server 2012 R2</u></p> <ol style="list-style-type: none"><li>1. ulepszenia edytora polityk grupowych</li><li>2. zmiany w zasadach przetwarzania polityk grupowych</li><li>3. nowe ustawienia GPO</li></ol> <p><u>Zarządzanie preferencjami Group Policy</u></p> <ol style="list-style-type: none"><li>1. przegląd zagadnień preferencji Group Policy</li><li>2. porównanie preferencji i polityk grupowych</li><li>3. konfiguracja ustawień preferencji</li><li>4. zaawansowana konfiguracja preferencji</li></ol>
Typ szkolenia	On-line w języku Polskim
Liczba uczestników	2 osoba
Czas trwania	Minimum 5 dni (40 godzin)
Certyfikat	Wymagany certyfikat lub zaświadczenie ukończenia szkolenia wydane przez jednostkę prowadzącą szkolenie.
Kontakt z trenerem po szkoleniu	14 dni