Załącznik nr 1 do umowy

(1.1) SZKOLENIA DLA PRACOWNIKÓW – BUDUJĄCE ŚWIADOMOŚĆ CYBERZAGROŻEŃ I SPOSOBÓW OCHRONY INFORMACJI (175 osób) 2024r.,2025r.,2026r.

Opis przedmiotu zamówienia (OPZ)

Zamawiający oczekuje realizacji szkoleń po jednym w każdym roku wdrożenia i trwania projektu Cyberbezpieczny Samorząd (2024r., 2025 r. i 2026r.). Szkolenia dla pracowników Urzędu **175 osób** budujące świadomość zagrożeń i sposobów ochrony informacji. Szkolenia realizowane przez trenerów w siedzibie Zamawiającego w godzinach pracy 7:30-15:30, wtorek 8:00-18:00, piątek 7:30-13:30 w formie zajęć stacjonarnych w miejscu wskazanym przez Zamawiającego.
Wszystkie opracowane materiały szkoleniowe, certyfikaty, harmonogramy, programy muszą zawierać informacje o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd" oraz logotypy **według wzoru przekazanego przez Zamawiającego**.
Zamawiający wymaga realizacji szkoleń według harmonogramów opracowanych przez Wykonawcę oraz dostarczonych Zamawiającemu przed rozpoczęciem szkolenia.
Zmawiający zastrzega sobie prawo wniesienia uwag do przedłożonego harmonogramu.
Zamawiający wymaga realizacji szkoleń, zgodnie z zaakceptowanym przez Zamawiającego, szczegółowym zakresem merytorycznym szkolenia, a opracowanym na podstawie ramowego programu szkolenia wskazanego przez Zamawiającego w niniejszym opisie przedmiotu zamówienia (Moduł 1 – Moduł 5).
Zamawiający wymaga opracowania i przekazania uczestnikom szkoleń materiałów szkoleniowych, obejmujących szczegółowy zakres szkolenia w formie elektronicznej (pliki .pdf), zawierających szczegółowe informacje, które będą omawiane podczas szkolenia.
Zamawiający nie dopuszcza metod zdalnych. Szkolenie w grupach nie większych niż **50 osób** (dla jednej grupy).

1. Termin realizacji szkoleń:
   1) **Pierwsze szkolenie w 2024 r. – w terminie do 14 dni** od dnia zawarcia umowy (**175 osób - grupy nie większe niż 50 osób** (kolejno po sobie lub rozłożone w ciągu 7-14 dni) **x 3 godziny zajęć/dzień** (jedna grupa). Jednostką czasową szkolenia jest 1 godzina szkoleniowa = 45 minut, przewiduje się dwie przerwy trwające po 10 minut w ciągu dnia).
   2) **Drugie szkolenie w 2025 r. - do dnia 29.08.2025 r. (175 osób - grupy nie większe niż 50 osób** (kolejno po sobie lub rozłożone w ciągu 7-14 dni) **x 3 godziny zajęć/dzień** (jedna grupa). Jednostką czasową szkolenia jest 1 godzina szkoleniowa = 45 minut, przewiduje się dwie przerwy trwające po 10 minut w ciągu dnia).
   3) **Trzecie szkolenie w 2026 r. - do dnia 20.02.2026 r. (175 osób - grupy nie większe niż 50 osób** (kolejno po sobie lub rozłożone w ciągu 7-14 dni) **x 3 godziny zajęć/dzień** (jedna grupa). Jednostką czasową szkolenia jest 1 godzina szkoleniowa = 45 minut, przewiduje się dwie przerwy trwające po 10 minut w ciągu dnia).

2. Zamawiający zapewni: salę szkoleniową, dostęp do sieci Internet, rzutnik, nagłośnienie.
3. Wykonawca będzie przestrzegał zasad równościowych podczas realizacji zamówienia, ze szczególnym uwzględnieniem przekazu równych szans kobiet i mężczyzn, informowania uczestników zajęć o współfinansowaniu projektu ze środków Unii Europejskiej.

Cel szkolenia: Podniesienie świadomości pracowników Urzędu w zakresie zagrożeń cyberbezpieczeństwa i sposobów ochrony informacji, zgodnie z najnowszymi zaleceniami CSIRT NASK, ENISA.

Grupa docelowa: Wszyscy pracownicy Urzędu, z uwzględnieniem specyfiki stanowisk i obowiązków (możliwe osobne moduły dla kadry kierowniczej i specjalistów IT).

1. **Moduł 1: Wprowadzenie do cyberbezpieczeństwa**

Podstawowe pojęcia i definicje: cyberbezpieczeństwo, zagrożenie, podatność, ryzyko, atak, incydent. Znaczenie cyberbezpieczeństwa dla Urzędu: skutki ataków cybernetycznych, odpowiedzialność prawna, ochrona danych osobowych, reputacja/wizerunek Urzędu.
Przegląd najnowszych trendów i zagrożeń w cyberprzestrzeni: w oparciu o raporty ENISA Threat Landscape (ETL) i raporty CERT Polska. Omówienie kluczowych obszarów cyberbezpieczeństwa: bezpieczeństwo sieci, bezpieczeństwo danych, bezpieczeństwo aplikacji, bezpieczeństwo urządzeń końcowych, bezpieczeństwo fizyczne, świadomość użytkowników.

2. **Moduł 2: Zagrożenia cybernetyczne i sposoby ochrony**

Zagrożenia związane z korzystaniem z Internetu: phishing, malware (wirusy, ransomware, spyware), strony internetowe podszywające się pod legalne serwisy, fałszywe wiadomości (fake news). Zagrożenia związane z pocztą elektroniczną: załączniki z złośliwym oprogramowaniem, phishing ukierunkowany (spear phishing), Business Email Compromise (BEC). Zagrożenia związane z mediami społecznościowymi: kradzież tożsamości, rozprzestrzenianie dezinformacji, inżynieria społeczna. Zagrożenia związane z urządzeniami mobilnymi: złośliwe aplikacje, kradzież danych, utrata urządzenia. Zagrożenia związane z pracą zdalną: zabezpieczenie sieci domowej, bezpieczne korzystanie z publicznych sieci Wi-Fi, ochrona danych na urządzeniach przenośnych.

3. **Moduł 3: Praktyczne zasady bezpieczeństwa**

Bezpieczne hasła: tworzenie silnych haseł, menedżery haseł, uwierzytelnianie wieloskładnikowe (MFA). Bezpieczne korzystanie z poczty elektronicznej: rozpoznawanie phishingu, ostrożność przy otwieraniu załączników, zasady bezpieczeństwa dla wiadomości poufnych. Bezpieczne przeglądanie stron internetowych: weryfikacja certyfikatów SSL, unikanie podejrzanych stron, aktualizacje oprogramowania. Bezpieczne korzystanie z mediów społecznościowych: ochrona prywatności, ostrożność przy publikowaniu informacji, weryfikacja źródeł informacji. Bezpieczne korzystanie z urządzeń mobilnych: instalacja oprogramowania antywirusowego, blokada ekranu, szyfrowanie danych, aktualizacje systemu. Bezpieczna praca zdalna: zabezpieczenie sieci domowej, VPN, zasady bezpieczeństwa dla wideokonferencji. Zasady czystego biurka i czystego ekranu: ochrona dokumentów papierowych i elektronicznych, blokada komputera po odejściu od stanowiska pracy. Zgłaszanie incydentów bezpieczeństwa: procedura zgłaszania incydentów, punkt kontaktowy ds. bezpieczeństwa.

4. **Moduł 4: Ochrona danych osobowych**

Podstawowe zasady RODO: legalność przetwarzania danych, celowość, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność, rozliczalność. Obowiązki pracowników w zakresie ochrony danych osobowych: poufność, zabezpieczenie danych, zgłaszanie naruszeń. Praktyczne aspekty ochrony danych osobowych w Urzędzie: przetwarzanie danych w systemach informatycznych, przechowywanie dokumentów, przekazywanie danych.

5. **Moduł 5: Zasady bezpieczeństwa informacji**

Klasyfikacja informacji w Urzędzie. Oznaczanie dokumentów: stopnie poufności, oznaczenia wizualne. Bezpieczne przechowywanie i archiwizowanie dokumentów: fizyczne zabezpieczenia, kontrola dostępu, niszczenie dokumentów. Bezpieczne przesyłanie informacji: szyfrowanie, bezpieczne kanały komunikacji.

Metody szkoleniowe:

Prezentacje multimedialne, Ćwiczenia praktyczne, Studia przypadków, Dyskusje, Quizy i testy wiedzy.

Zamawiający zastrzega, że agenda może być modyfikowana przez Zamawiającego w zależności od aktualnych potrzeb i specyfiki Urzędu oraz zakresu wdrożonego SZBI na każdym etapie realizacji zadania.

Szkolenia powinny być prowadzone przez wykwalifikowanych specjalistów ds. cyberbezpieczeństwa potwierdzone stosowną dokumentacją.

Po zakończonym szkoleniu Wykonawca przygotuje i przeprowadzi test kompetencji.

Wykonawca po pozytywnym zaliczeniu przez uczestników końcowego testu kompetencji wystawi potwierdzenie odbycia szkolenia w postaci imiennego certyfikatu dla każdego z uczestników – Wykonawca przekaże certyfikaty potwierdzające udział w szkoleniu do uzupełnienia o dane uczestników przez Zleceniodawcę.

Szkolenie musi być na każdym etapie zgodne z zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn.

(1.2) SZKOLENIA SPECJALISTYCZNE DLA INFORMATYKÓW W ZAKRESIE ZASTOSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA (3 osoby) 2024r.,2025r.,2026r.

Opis przedmiotu zamówienia (OPZ)

Zamawiający wymaga zorganizowania szkolenia dla 3 pracowników działu IT z zakresu Administrowania systemem Windows Server, Zarządzania usługą Active Directory w środowisku Microsoft Windows Server 2019/2022 oraz Wirtualizacji Hyper-V, magazynowania i przetwarzania danych w środowisku Microsoft Windows Server 2019/2022. **Szkolenia będą realizowane przez 3 lata, jedno w roku 2024, kolejne w roku 2025 i ostatnie w 2026 roku**. Wykonawca musi zagwarantować szkolenia spełniające minimum poniższe agendy.

I. Agenda szkolenia Administrowanie systemem Windows Server:

1. Wprowadzenie do administracji systemu Windows Server
   1) Wprowadzenie do systemu Windows Server.
   2) Wprowadzenie do systemu Windows Server Core.
   3) Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server.
2. Usługi zarządzania tożsamością w systemie Windows Server
   1) Wprowadzenie do AD DS.
   2) Wdrażanie kontrolerów domeny Windows Server.
   3) Wprowadzenie do usługi Azure AD.
   4) Wdrażanie zasad grupy.
   5) Wprowadzenie do usług certyfikatów Active Directory.
3. Usługi infrastruktury sieciowej w systemie Windows Server
   6) Wdrażanie i zarządzanie protokołem DHCP.
   7) Wdrażanie i zarządzanie systemem DNS.
   8) Wdrażanie i zarządzanie systemem IPAM.
   9) Usługi dostępu zdalnego w systemie Windows Server.
4. Serwery plików i zarządzanie pamięcią masową w systemie Windows Server
   1) Woluminy i systemy plików w systemie Windows Server.
   2) Wdrażanie udostępniania w systemie Windows Server.
   3) Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server.
   4) Wdrażanie deduplikacji danych.
   5) Wdrażanie interfejsu Iscsi.
   6) Wdrażanie rozproszonego systemu plików.
5. Wirtualizacja Hyper-V i kontenery w systemie Windows Server
   1) Hyper-V w systemie Windows Server.
   2) Konfiguracja maszyn wirtualnych.
   3) Zabezpieczanie wirtualizacji w systemie Windows Server.
   4) Kontenery w systemie Windows Server.
   5) Wprowadzenie do platformy Kubernetes.
6. Wysoka dostępność w systemie Windows Server
   1) Planowanie wdrożenia klastra pracy awaryjnej.
   2) Tworzenie i konfiguracja klastra pracy awaryjnej.
   3) Wprowadzenie do rozciągniętych klastrów.

4) Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V.

7. Odzyskiwanie danych po awarii w systemie Windows Server
   1) Funkcja Hyper-V Replica.
   2) Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server.
8. Bezpieczeństwo systemu Windows Server
   1) Ochrona danych uwierzytelniających i dostępu uprzywilejowanego.
   2) Hardening systemu Windows Server.
   3) JEA w systemie Windows Server.
   4) Zabezpieczanie i analiza ruchu w SMB.
   5) Zarządzanie aktualizacjami w systemie Windows Server.
9. RDS (usługi pulpitu zdalnego) w systemie Windows Server
   1) Wprowadzenie do RDS.
   2) Konfiguracja wdrażania pulpitu opartego na sesji.
   3) Wprowadzenie do osobistych i połączonych pulpitów wirtualnych.
10. Dostęp zdalny i usługi internetowe w systemie Windows Server
    1) Wdrażanie sieci VPN.
    2) Wdrażanie usługi Always On VPN.
    3) Wdrażanie systemu NPS.
    4) Wdrażanie serwera WWW w systemie Windows Server.
11. Monitorowanie serwera i wydajności w systemie Windows Server
    1) Wprowadzenie do narzędzi do monitorowania systemu Windows Server.
    2) Korzystanie z monitora wydajności.
    3) Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów.
12. Aktualizacja i migracja w systemie Windows Server
    1) Migracja AD DS.
    2) Usługa migracji pamięci masowej.
    3) Narzędzia do migracji systemu Windows Server.

II. Agenda szkolenia Zarządzanie usługą Active Directory w środowisku Microsoft Windows Server 2019/2022:

1. Instalacja i konfiguracja kontrolerów domeny
   1) Omówienie usług AD DS.
   2) Omówienie kontrolerów domeny usług AD DS.
   3) Wdrożenie kontrolera domeny.
   4) Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022.
2. Zarządzanie obiektami w AD DS.
   1) Zarządzanie kontami użytkowników.
   2) Zarządzanie grupami w usługach AD DS.
   3) Zarządzanie obiektami typu komputer w AD DS.
   4) Wdrażanie i zarządzanie OU.
3. Zarządzanie zaawansowaną infrastrukturą AD DS.
   1) Wprowadzenie do zaawansowanych wdrożeń AD DS.
   2) Wdrożenie rozproszonego środowiska AD DS.
   3) Konfiguracja relacji zaufania AD DS.
4. Wdrażanie i zarządzanie lokacjami i repliką AD DS.
   1) Omówienie replikacji usług AD DS.

2) Konfigurowanie lokacji usług AD DS.
3) Konfigurowanie i monitorowanie replikacji usług AD DS.

5. Wdrażanie zasad grupy
1) Wprowadzenie do zasad grupy.
2) Wdrażanie i zarządzanie obiektami GPO (Group Policy Object).
3) Konfiguracja zakresu i przetwarzania obiektów GPO.
4) Rozwiązywanie problemów z GPO.

6. Zarządzanie ustawieniami użytkowników za pomocą zasad grupy
1) Wdrażanie szablonów administracyjnych.
2) Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów.
3) Konfiguracja preferencji zasad grupowych.

III. Agenda szkolenia: Wirtualizacja Hyper-V, magazynowanie i przetwarzanie danych w środowisku Microsoft Windows Server 2019/2022:

1. Omówienie funkcji administracyjnych systemu Windows Server
1) Informacje wstępne o systemie Windows Server 2019.
2) Omówienie najważniejszych funkcji systemu Windows Server.
3) Omówienie zasad i narzędzi związanych z zarządzaniem systemem Windows Server.

2. Zarządzanie serwerami plików i pamięcią masową w systemie Windows Server
1) Wolumeny i systemy plików w systemie Windows Server.
2) Współużytkowanie zasobów w systemie Windows Server.
3) Wdrażanie obszarów pamięci masowej w systemie Windows Server.
4) Wdrażanie funkcji deduplikacji danych.
5) Wdrażanie protokołu ISCSI.
6) Wdrażanie rozproszonego systemu plików.
7) Migracja magazynu danych w Windows Server 2022.

3. Oprogramowanie do wirtualizacji Hyper-V i kontenery w systemie Windows Server
1) Hyper-V w systemie Windows Server.
2) Konfigurowanie maszyn wirtualnych.
3) Zabezpieczenie wirtualizacji w systemie Windows Server.
4) Ulepszenia działania wirtualnego przełącznika sieciowego w Windows Server 2022.
5) Kontenery w systemie Windows Server.

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

5. Usuwanie skutków awarii w systemie Windows Server
1) Funkcja Hyper-V Replica.
2) Infrastruktura tworzenia i odtwarzania kopii zapasowych w systemie Windows Server.

6. Implementowanie i zarządzanie zasobami typu failover clustering
1) Planowanie strategii wdrożenia typu failover cluster.
2) Tworzenie i konfiguracja struktury failover cluster.

3) Monitoring infrastruktury.

7. Implementowanie rozwiązań typu failover clustering dla maszyn wirtualnych w Hyper-V
   1) Prezentacja i integracja Hyper-V w Windows Server 2016 wraz z failover clustering.
   2) Implementacja i zarządzanie maszynami wirtualnymi w Hyper-V w failover clusters.
   3) Główne cechy wdrożeń maszyn wirtualnych w środowisku typu wysokiej dostępności i niezawodności.
   4) Szyfrowane Cluster Shared Volumes w Windows Server 2022.
8. Implementowanie network load balancing
   1) Przegląd metod zastosowania klastrów typu NLB.
   2) Konfiguracja klastrów NLB.
   3) Planowanie i implementacja NLB.