

**Wykonanie audytu cyberbezpieczeństwa oraz zakup szkoleń w ramach projektu****pn.: „Wdrożenie e-usług w Szpitalu Powiatowym w Rawiczu Sp. z o.o.”****- Nr postępowania NLO-3822-01/TP/26****OPIS PRZEDMIOTU ZAMÓWIENIA****CZĘŚĆ NR 1** – Wykonanie audytu cyberbezpieczeństwa**I. PRZEDMIOT ZAMÓWIENIA**

1. Audyt obejmuje analizę, w szczególności:
  - infrastruktury sieciowej (LAN/WAN, Wi-Fi, firewall, VPN),
  - serwerów fizycznych i wirtualnych,
  - stacji roboczych i urządzeń mobilnych,
  - systemów operacyjnych i baz danych,
  - systemów kopii zapasowych i odtwarzania danych,
  - systemów klasy HIS/ERP oraz innych systemów krytycznych,
  - zabezpieczeń antywirusowych i EDR,
  - mechanizmów logowania i monitoringu.
2. Testy bezpieczeństwa: W ramach audytu Wykonawca przeprowadzi, w zakresie uzgodnionym z Zamawiającym:
  - testy podatności (vulnerability assessment),
  - analizę konfiguracji systemów i urządzeń,
  - analizę odporności na wybrane scenariusze ataków,z wyłączeniem testów powodujących przerwy w pracy systemów lub ryzyko utraty danych.
3. W ramach zamówienia Wykonawca dostarczy:
  - 1) Raport z audytu cyberbezpieczeństwa, zawierający co najmniej:
    - opis stanu obecnego,
    - listę zidentyfikowanych podatności i zagrożeń,
    - ocenę poziomu ryzyka (niski/średni/wysoki),
    - ocenę dojrzałości cyberbezpieczeństwa,
    - wnioski i podsumowanie.
  - 2) Plan działań naprawczych, zawierający:
    - rekomendowane środki techniczne i organizacyjne,
    - priorytety wdrożeń,
    - szacunkową pracochłonność,
    - rekomendowaną kolejność realizacji.
  - 3) Prezentację wyników audytu dla kierownictwa Zamawiającego.

**II. WYMAGANIA ORGANIZACYJNE I TECHNICZNE**

1. Termin końcowy: Całość przedmiotu zamówienia musi zostać zrealizowana i odebrana do dnia 26.05.2026r.
2. Oznakowanie: Wykonawca zobowiązany jest do oznakowania materiałów i certyfikatów logotypami KPO i UE.

## **CZĘŚĆ NR 2** - Realizacja specjalistycznych szkoleń IT w obszarach cyberbezpieczeństwa, baz danych oraz programowania w języku Python.

### **I. PRZEDMIOT ZAMÓWIENIA**

1. Przedmiotem zamówienia jest usługa polegająca na przygotowaniu i kompleksowym przeprowadzeniu cyklu specjalistycznych szkoleń z zakresu SZBI, PBI oraz cyberbezpieczeństwa dla pracowników Zamawiającego, obejmująca również aktualizację systemu zarządzania bezpieczeństwem informacji oraz polityk bezpieczeństwa informacji.
2. Przedmiot zamówienia dotyczy realizacji specjalistycznych szkoleń dla kadry IT, kadry kierowniczej, biurowej oraz medycznej w co najmniej 75% pracowników pracujących na systemach informatycznych szpitala w obszarach cyberbezpieczeństwa, baz danych oraz programowania w języku Python.
3. Zamówienie obejmuje trzy główne obszary: Cyberbezpieczeństwo (z AD), Bazy Danych oraz Programowanie w języku Python.

### **II. SZCZEGÓŁOWY ZAKRES TEMATYCZNY**

1. Obszar: Cyberbezpieczeństwo i Etno-hacking dla kadry IT,  
Celem szkolenia jest zapoznanie uczestników z aktualnymi zagrożeniami w cyberprzestrzeni oraz metodami ofensywnego testowania bezpieczeństwa systemów IT. Zakres obejmuje:
  - Podstawy etycznego hackingu: wprowadzenie do metodyki testów penetracyjnych, aspekty prawne oraz etyczne.
  - Rekonesans i skanowanie: techniki zbierania informacji o celach (OSINT), skanowanie sieci, identyfikacja usług i wersji systemów.
  - Techniki ataku i eksploatacji: ataki na poziomie sieciowym (Sniffing, MITM), eskalacja uprawnień, techniki przejmowania kontroli nad stacjami roboczymi i serwerami.
  - Ataki na aplikacje i hasła: łamanie zabezpieczeń uwierzytelniania, socjotechnika oraz analiza podatności typu Zero-day.
2. Obszar: Tożsamość i Usługi Katalogowe (Windows Server) dla kadry IT,  
Szkolenie koncentruje się na zaawansowanym zarządzaniu tożsamością w infrastrukturze opartej o Active Directory. Zakres obejmuje:
  - Active Directory Domain Services (AD DS): instalacja, konfiguracja i zaawansowane administrowanie obiektami domenowymi oraz kontrolerami domeny.
  - Zarządzanie Certyfikatami i Federacją: wdrażanie usług AD Certificate Services (AD CS) oraz infrastruktury AD Federation Services (AD FS) dla bezpiecznego dostępu do aplikacji.
  - Ochrona Tożsamości: implementacja mechanizmów uwierzytelniania wieloskładnikowego (MFA), zarządzanie kontami uprzywilejowanymi oraz synchronizacja z usługami hybrydowymi.
3. Obszar: Administracja Systemowa (Windows Server) dla kadry IT,  
Zakres obejmuje kluczowe aspekty utrzymania i optymalizacji środowisk serwerowych. Szczegółowa tematyka to:
  - Usługi Sieciowe i IPAM: zarządzanie adresacją IP, usługami DNS oraz DHCP w skali przedsiębiorstwa.

- Pamięć masowa i Wirtualizacja: konfiguracja Storage Spaces Direct (S2D), wdrażanie klastrów wysokiej dostępności (Failover Clustering) oraz zarządzanie maszynami wirtualnymi i kontenerami.
- Utrzymanie i Monitoring: analiza wydajności systemu, optymalizacja usług serwerowych oraz procedury Backup & Disaster Recovery.

4. Obszar: Relacyjne Bazy Danych (SQL) dla kadry IT,

Szkolenie przygotowuje do samodzielnej pracy z bazami danych w zakresie ich projektowania i odpytywania. Zakres obejmuje:

- Modelowanie Danych: projektowanie struktur tabel, definiowanie relacji, kluczy głównych (Primary Key) i obcych (Foreign Key) oraz normalizacja bazy danych.
- Język Zapytań SQL: budowanie zapytań wybierających (SELECT), filtrowanie danych, sortowanie oraz łączenie tabel przy użyciu różnych typów złączeń (JOIN).
- Przetwarzanie i Agregacja: stosowanie funkcji agregujących, grupowanie wyników, operacje na zbiorach oraz tworzenie podzapytań i widoków.
- Manipulacja danymi i programowanie: instrukcje INSERT, UPDATE, DELETE oraz podstawy tworzenia procedur składowanych i funkcji bazodanowych.

4. Obszar: szkolenie kadry kierowniczej – w zakresie:

- Podstaw prawnych w obszarze cyberbezpieczeństwa
- Typów ataków
- Reagowania na incydenty
- Wykonywania badań bezpieczeństwa
- Roli kadry zarządzającej w procesach bezpieczeństwa

5. Obszar: szkolenie kadry biurowej oraz medycznej – w zakresie:

- Podstawowych zasad cyberhigieny
- Typów ataków wraz z przykładami
- Reagowania na incydenty

### **III. WYMAGANIA ORGANIZACYJNE I TECHNICZNE**

1. Tryb realizacji: Preferowany tryb zdalny (online) w czasie rzeczywistym z trenerem.
2. Laboratoria: Wykonawca zapewni dostęp do indywidualnych środowisk laboratoryjnych dla każdego uczestnika (maszyny wirtualne/chmura).
3. Język: Szkolenia i materiały w języku polskim (dopuszczalne materiały techniczne w j. angielskim).
4. Po każdym szkoleniu powinien być zagwarantowany minimum 14-sto dniowy, mailowy kontakt z trenerem.

### **IV. CERTYFIKACJA I WERYFIKACJA WIEDZY**

1. Każde szkolenie musi zakończyć się wydaniem imiennego certyfikatu (autoryzowanego przez producenta, zewnętrznego lub autorskiego wykonawcy) dla kadry IT.
2. Egzamin zewnętrzny nie jest wymagany, jednak Wykonawca zobowiązany jest do przeprowadzenia testów sprawdzających przyrost wiedzy (pre-test i post-test) zgodnie z wymogami KPO.

## **V. TERMINY I FINANSOWANIE**

4. Termin końcowy: Całość przedmiotu zamówienia musi zostać zrealizowana i odebrana do dnia 26.05.2026 r.
5. Oznakowanie: Wykonawca zobowiązany jest do oznakowania materiałów i certyfikatów logotypami KPO i UE.