GMINA ŚWIDNICA

OPIS PRZEDMIOTU ZAMÓWIENIA

Znak sprawy: ZOI.271.1.2026

Świdnica, dnia 23-01-2026 r.

Zamawiający:
Gmina Świdnica
ul. B. Głowackiego 4,
58-100, Świdnica
NIP: 8842365226
REGON: 890718389

ZAPYTANIE OFERTOWE

Gmina Świdnica zaprasza do składania ofert na wykonanie zadania o wartości szacunkowej nieprzekraczającej kwoty 130 tys. PLN (zwolnione ze stosowania ustawy Pzp na podstawie art.2 ust.1 pkt 1 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych - tekst jednolity Dz.U. z 2021 r. poz. 1129 z późn. zm.) pn.: „Realizacja specjalistycznych szkoleń z zakresu cyberbezpieczeństwa dla pracowników, kadry IT oraz kadry zarządzającej Urzędu Gminy Świdnica", realizowanego w ramach Projektu „Cyberbezpieczny Samorząd".

Projekt finansowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021 — 2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, projekt grantowy „Cyberbezpieczny Samorząd", zgodnie z wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2021-2027.

Bartłomiej Strózik
Elektronicznie podpisany przez Bartłomiej Strózik
Data: 2026.01.23 13:42:35 +01'00'

.....
Zatwierdził Wójt Gminy

I. Informacje o projekcie

Zamówienie jest finansowane w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021 - 2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, projekt grantowy „Cyberbezpieczny Samorząd".

II. Miejsce publikacji zapytania. Komunikacja z Zamawiającym

1. Ofertę należy złożyć przesyłając ją poprzez platformę e-Doręczeń na adres Urzędu Gminy w Świdnicy: AE:PL-67264-75623-FBDDU-15 do dnia 02.02.2026 do godz.12:00.

2. Do oferty należy dołączyć formularz ofertowo-cenowy zgodny z załącznikiem nr 1 niniejszego zapytania ofertowego pod rygorem nieważności oferty.

3. Wykonawca ponosi wszystkie koszty związane z przygotowaniem i złożeniem oferty.

4. Oferta powinna być napisana w języku polskim, trwałą i czytelną techniką.

5. Oferta powinna zawierać: wypełniony i podpisany formularz ofertowy wraz z oświadczeniami.

6. Formularz ofertowy oraz oświadczenia muszą zostać podpisane przez osobę/osoby uprawnione do reprezentowania Wykonawcy (zgodnie z formą reprezentacji określoną w rejestrze handlowym lub innym dokumencie właściwym dla formy organizacji wykonawcy). Podpis musi zostać złożony w formie elektronicznej (kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty), zgodnie z wymogami określonymi w Rozdziale IX niniejszego Zapytania.

III. Rodzaj zamówienia

Niniejsze zamówienie jest zamówieniem na usługi

IV. Kody CPV

a. 80000000-4 - Usługi edukacyjne i szkoleniowe
b. 80511000-9 - Usługi szkolenia personelu
c. 80533100-0 - Usługi szkolenia komputerowego
d. 80533000-9 - Usługi zapoznawania użytkownika z obsługą komputera i usługi szkoleniowe
e. 80550000-4 - Usługi szkolenia w dziedzinie bezpieczeństwa

V. Przebieg postępowania

1. Zamawiający zastrzega sobie możliwość dokonania zmian w niniejszym Zapytaniu przed upływem terminu składania ofert.

2. W przypadku wprowadzenia zmian Zamawiający udostępni informację o zmianach na stronie internetowej prowadzonego postępowania.

3. Zamawiający może w toku badania i oceny ofert żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz uzupełnienia dokumentów i oświadczeń, jeżeli takie były wymagane.

4. Zamawiający odrzuci ofertę, która:

    a. nie spełnia wymagań określonych w niniejszym Zapytaniu ofertowym,

    b. zawiera błędy w obliczeniu ceny - Zamawiający może poprawić w treści oferty oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe oraz inne omyłki polegające na niezgodności oferty z wymaganiami Zamawiającego, niepowodujące istotnych zmian w treści oferty - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona; w przypadku poprawienia innej omyłki polegającej na niezgodności oferty z wymaganiami Zamawiającego, niepowodującej istotnych zmian w treści oferty, oferta Wykonawcy podlega odrzuceniu, jeżeli Wykonawca nie wyrazi zgody na poprawienie oferty w terminie określonym przez Zamawiającego,

    c. zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia,

    d. jest nieważna na podstawie odrębnych przepisów.

5. Zamawiający zastrzega sobie, że:

    a. ma prawo unieważnienia postępowania, w przypadku wystąpienia istotnej zmiany okoliczności powodującej, że prowadzenie postępowania lub wykonanie przedmiotu zamówienia nie leży w interesie Zamawiającego, czego nie można było wcześniej przewidzieć;

    b. ma prawo unieważnienia postępowania, jeżeli jest ono obarczone niemożliwą do usunięcia wadą uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie niniejszego zamówienia;

    c. może unieważnić postępowanie, gdy nie złożono żadnej oferty lub wszystkie złożone oferty będą podlegały odrzuceniu lub koszt najkorzystniejszej oferty lub oferta z najniższą ceną przewyższać będzie kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, przy czym Zamawiający zastrzega, iż może rozważyć zwiększenie kwoty, którą zamierza przeznaczyć na sfinansowanie zamówienia, jednak Wykonawcy nie będą mieli roszczenia o zwiększenie tej kwoty;

    d. ma prawo unieważnić całe lub część postępowania w sytuacji, gdy nie pozyska lub utraci źródło finansowania wskazane we wstępie niniejszego zapytania lub nastąpi zmiana zasad przyznawania lub rozliczania tego finansowania.

6. Wybór oferty i przekazanie przez Zamawiającego informacji o wyborze oferty nie stanowi przyjęcia oferty w rozumieniu Kodeksu cywilnego i nie oznacza zobowiązania do zawarcia umowy pomiędzy Zamawiającym i Wykonawcą.

7. Zawarcie umowy z wybranym Wykonawcą nastąpi w miejscu i terminie wyznaczonym przez Zamawiającego.

8. Jeżeli Wykonawca, którego oferta została wybrana uchyla się od zawarcia umowy, Zamawiający może wybrać najkorzystniejszą ofertę spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.

9. Niezwłocznie po zakończeniu postępowania zawiadamia się wszystkich Wykonawców, którzy złożyli oferty, o wyborze najkorzystniejszej oferty lub o unieważnieniu postępowania. W

przypadku wyboru oferty najkorzystniejszej wskazuje się co najmniej imię i nazwisko lub nazwę (firmę) oraz adres Wykonawcy, którego ofertę wybrano oraz cenę wybranej oferty.

10. Złożenie oferty oznacza zaakceptowanie przez Wykonawcę wymagań zawartych w niniejszym Zapytaniu oraz zaakceptowanie ich bez zastrzeżeń.

VI. Opis przedmiotu zamówienia

1. Informacje wstępne

Do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu o udzielenie zamówienia publicznego nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz.U. z 2024 r., poz. 1320 t.j. z póź. zm – dalej jako „pzp").

1) Oznaczenie postępowania: postępowanie posiada znak sprawy. Zaleca się, aby Wykonawcy we wszelkich kontaktach z Zamawiającym powoływali się na wyżej wskazane oznaczenie.

2) Postępowanie prowadzone jest w oparciu o wytyczne Reguły Konkurencyjności.

3) Postępowanie prowadzone jest w języku polskim.

Przedmiotem zamówienia jest kompleksowe przeprowadzenie specjalistycznych szkoleń z zakresu cyberbezpieczeństwa dla pracowników, kadry IT oraz kadry zarządzającej Zamawiającego. Wszystkie szkolenia muszą zostać zrealizowane w terminie do 31 maja 2026 roku.

Część 1 – Zaawansowane szkolenia dla kadry IT

Przedmiotem tej części zamówienia jest usługa przeprowadzenia zaawansowanych szkoleń w formie online dla **2 (dwóch)** pracowników Zamawiającego. Celem szkoleń jest zdobycie praktycznych umiejętności w zakresie zaawansowanych funkcji SIEM, automatyzacji reakcji na incydenty (SOAR), detekcji zagrożeń oraz wykorzystania Threat Intelligence.

1. **Szkolenie nr 1 – Wprowadzenie do cyberbezpieczeństwa. Podstawy bezpieczeństwa sieciowego. Narzędzia Windows oraz Linux (zdalne)**

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne**	
1.1	Nazwa szkolenia	Wprowadzenie do cyberbezpieczeństwa. Podstawy bezpieczeństwa sieciowego. Narzędzia dla systemów Windows oraz Linux.
1.2	Forma	Szkolenie może być przeprowadzone w formie zdalnej (online), prowadzonej na żywo przez instruktora.
1.3	Czas trwania	Szkolenie musi obejmować minimum 1 dzień, co stanowi łącznie co najmniej 7 godzin zajęć dydaktycznych. Szkolenie musi zostać zrealizowane nie później niż do 31.05.2026 r.
1.4	Język	Szkolenie oraz wszystkie materiały muszą być w języku polskim.
1.7	Instruktor	Szkolenie musi być prowadzone przez trenera z praktycznym doświadczeniem w obszarze cyberbezpieczeństwa defensywnego (np. inżyniera SOC).

2.	**Zakres Merytoryczny**	
2.1	Wprowadzenie do cyberbezpieczeństwa	Temat szkolenia musi obejmować: ścieżki rozwoju i certyfikacje w branży, rolę zespołów Blue Team/SOC, wymagane kompetencje rynkowe.
2.2	Podstawowe usługi sieciowe	Temat szkolenia musi obejmować: omówienie kluczowych protokołów (HTTP, HTTPS, FTP, SMB, RDP), podstawowych portów, podstaw sieci (IP, subnetting, NAT, DNS, DHCP, VPN) oraz praktyczne laboratoria ze skanowania i analizy usług.
2.3	Narzędzia i Komendy w Windows oraz Linux	Temat szkolenia musi obejmować: praktyczne wykorzystanie komend i narzędzi w systemach Windows i Linux do monitorowania, analizy i testów bezpieczeństwa, w tym ćwiczenia z wykrywania luk w usługach.
2.4	Wirtualizacja	Temat szkolenia musi obejmować: zastosowanie maszyn wirtualnych (VM) do tworzenia bezpiecznych, izolowanych środowisk testowych do analizy zagrożeń; stworzenie i zarządzanie maszynami wirtualnymi.
3.	**Materiały i Usługi w cenie**	
3.1	Materiały szkoleniowe	Wykonawca dostarczy Zamawiającemu komplet materiałów dydaktycznych w formie elektronicznej lub papierowej.
3.2	Zaświadczenie o ukończeniu	Wykonawca zapewni Zamawiającemu imienne zaświadczenie o ukończeniu szkolenia.
3.3	Wsparcie poszkoleniowe	Wykonawca jest zobowiązany zapewnić Zamawiającemu możliwość kontaktu z trenerem w celach merytorycznych przez okres co najmniej 14 dni po zakończeniu szkolenia.

2. Szkolenie nr 2 – Analiza Logów i ruchu sieciowego. IT Monitoring & Hardening (zdalne)

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne**	
1.1	Nazwa szkolenia	Analiza Logów i ruchu sieciowego. IT Monitoring & Hardening.
1.2	Forma	Szkolenie może być przeprowadzone w fodrmie zdalnej (online), prowadzonej na żywo przez instruktora.
1.3	Czas trwania	Szkolenie musi obejmować minimum 1 dzień, co stanowi łącznie co najmniej 7 godzin zajęć dydaktycznych i musi się zakończyć do dnia 31.05.2026 r.
1.4	Język	Szkolenie oraz wszystkie materiały muszą być w języku polskim.
1.5	Instruktor	Szkolenie musi być prowadzone przez trenera z praktycznym doświadczeniem w obszarze cyberbezpieczeństwa defensywnego (np. inżyniera SOC).
2.	**Zakres Merytoryczny**	
2.1	Wprowadzenie	Temat szkolenia musi obejmować: znaczenie monitorowania systemów, rolę logów w cyberbezpieczeństwie, wykrywanie nieautoryzowanego dostępu, monitorowanie aplikacji i reakcje na zdarzenia.

2.2	Windows - Monitorowanie i analiza logów	Temat szkolenia musi obejmować: monitorowanie aktywności użytkowników i aplikacji w Windows, analizę logów w Podglądzie zdarzeń (Security, Application) oraz podstawowe komendy CMD i PowerShell.
2.3	Linux - Monitorowanie i analiza logów	Temat szkolenia musi obejmować: analizę podstawowych logów systemowych (np. /var/log/auth.log, /var/log/syslog), monitorowanie działań użytkowników oraz podstawowe komendy i narzędzia analityczne.
2.4	Hardening systemów	Temat szkolenia musi obejmować: zasady utwardzania systemów Windows i Linux, najlepsze praktyki w zabezpieczaniu usług, podstawowe komendy sieciowe (np. ping, tracert, netstat, tcpdump) oraz analizę ruchu sieciowego (np. Wireshark).
2.5	AV/EDR - Analiza logów i wykrywanie zagrożeń	Temat szkolenia musi obejmować: wprowadzenie do narzędzi klasy EDR (Endpoint Detection and Response), analizę logów z EDR, interpretację zdarzeń bezpieczeństwa w logach antywirusowych oraz praktyczne ćwiczenia w identyfikacji zagrożeń.
3.	**Materiały i Usługi w cenie**	
3.1	Materiały szkoleniowe	Wykonawca dostarczy Zamawiającemu komplet materiałów dydaktycznych w formie elektronicznej lub papierowej.
3.2	Certyfikat/Zaświadczenie	Wykonawca zapewni Zamawiającemu imienne zaświadczenie o ukończeniu szkolenia, z opcją uzyskania certyfikatu po zdaniu egzaminu.
3.3	Egzamin	Wykonawca zapewni możliwość przystąpienia do egzaminu końcowego – potwierdzającego zdobytą wiedzę.
3.4	Wsparcie poszkoleniowe	Wykonawca jest zobowiązany zapewnić Zamawiającemu możliwość kontaktu z trenerem w celach merytorycznych przez okres co najmniej 14 dni po zakończeniu szkolenia.

3. Szkolenie nr 3 – Zawansowane bezpieczeństwo infrastruktury. Active Directory. Systemy zabezpieczeń sieciowych (zdalne)

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne**	
1.1	Nazwa szkolenia	Zawansowane bezpieczeństwo infrastruktury. Active Directory. Systemy zabezpieczeń sieciowych.
1.2	Forma	Szkolenie odbywa się w formule zdalnej (online) lub stacjonarnej.
1.3	Czas trwania	Szkolenie musi obejmować minimum 2 dni, co stanowi łącznie co najmniej 14 godzin zajęć dydaktycznych.
1.4	Język	Szkolenie oraz wszystkie materiały muszą być w języku polskim.
1.5	Instruktor	Szkolenie musi być prowadzone przez trenera z praktycznym doświadczeniem w obszarze cyberbezpieczeństwa defensywnego.
2.	**Zakres Merytoryczny**	

2.1	Moduł 1: Active Directory	Zakres szkolenia musi obejmować: Struktura i mechanizmy AD (LDAP, Kerberos, NTLM). Ataki na AD (Pass-the-Hash, Kerberoasting). Obrona i hardening AD (GPO, LAPS, monitorowanie logów).
2.2	Moduł 2: Firewall, IDS/IPS, WAF & UTM	Zakres szkolenia musi obejmować: Konfigurację firewalli. IDS/IPS (analiza ruchu, tuning reguł). WAF (zabezpieczenie aplikacji webowych). UTM (ochrona wielowarstwowa i zarządzanie zagrożeniami).
2.3	Moduł 3: IAM, PAM, DLP & Backup	Zakres szkolenia musi obejmować: IAM (zarządzanie tożsamościami i dostępem). PAM (ochrona kont uprzywilejowanych). DLP (zabezpieczenie przed wyciekiem danych). Backup i odzyskiwanie danych po ataku ransomware.
3.	**Materiały i Usługi w cenie**	
3.1	Egzamin	Wykonawca zobowiązany jest w ramach oferowanej ceny do zapewnienia, opłacenia i organizacji egzaminu końcowego potwierdzającego zdobytą wiedzę.
3.2	Materiały i Certyfikacja	Wykonawca dostarczy materiały dydaktyczne. Wykonawca zapewni zaświadczenie o ukończeniu szkolenia.
3.3	Wsparcie poszkoleniowe	Wykonawca jest zobowiązany zapewnić możliwość kontaktu z trenerem w celach merytorycznych.
3.4	Praktyka	Szkolenie opiera się na praktycznych laboratoriach opartych na realnych zagrożeniach.

4. Szkolenie nr 4 – Detekcja, Reagowanie i Automatyzacja w SOC L1 (zdalne)

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne**	
1.1	Nazwa szkolenia	Detekcja, Reagowanie i Automatyzacja w SOC L1.
1.2	Forma	Szkolenie może być przeprowadzone w formie zdalnej (online), prowadzonej na żywo przez instruktora.
1.3	Czas trwania	Szkolenie musi obejmować minimum 1 dzień, co stanowi łącznie co najmniej 7 godzin zajęć dydaktycznych i musi się zakończyć do dnia 31.05.2026 r..
1.4	Język	Szkolenie oraz wszystkie materiały muszą być w języku polskim.
1.5	Instruktor	Szkolenie musi być prowadzone przez trenera z praktycznym doświadczeniem w obszarze cyberbezpieczeństwa defensywnego (np. inżyniera SOC).
2.	**Zakres Merytoryczny**	
2.1	Analiza logów i SIEM	Zakres szkolenia musi obejmować: Wprowadzenie do funkcji i architektury SIEM, Rola SIEM w SOC L1, Analiza i korelacja zdarzeń z logów, Źródła logów (Windows Event Logs, Sysmon, firewall).
2.2	Frameworki Detekcji	Zakres szkolenia musi obejmować: Rola frameworków w detekcji zagrożeń, MITRE ATT&CK, Sigma, YARA, Proces detekcja zagrożeń.

2.3	Incident Response (IR) i Eskalacja	Zakres szkolenia musi obejmować: Eskalację alertów i triage (5-punktowa checklista L1), Etapy reagowania na incydent (wg NIST), Automatyzacja: auto-close, tagging, playbooki.
2.4	Automatyzacja Reakcji (SOAR)	Zakres szkolenia musi obejmować: Architektura SOAR (Shuffle), Scenariusze automatyzacji (phishing, ransomware, hash checking), Integracja z Elastic, VirusTotal, HybridAnalysis.
2.5	Threat Intelligence (TI)	Zakres szkolenia musi obejmować: TI jako źródło kontekstu (hash, IP, domena), Korelacja IoC w SIEM, Narzędzia (VirusTotal, OTX, MISP).
2.6	Scenariusze i Narzędzia	Szkolenie opiera się na realistycznych scenariuszach ataków: brute-force, phishing, ransomware oraz APT. Wykorzystuje narzędzia takie jak Elastic Stack, Shuffle, MISP, VirusTotal i inne.
3.	**Materiały i Usługi w cenie**	
3.1	Materiały i Środowisko	Wykonawca dostarczy Zamawiającemu komplet materiałów dydaktycznych. Uczestnicy analizują prawdziwe logi z Windows, Linux, firewalli i EDR.
3.2	Certyfikat/Zaświadczenie	Wykonawca zapewni Zamawiającemu imienne zaświadczenie o ukończeniu szkolenia, z opcją uzyskania certyfikatu po zdaniu egzaminu.
3.3	Egzamin	Wykonawca zobowiązany jest w ramach oferowanej ceny do zapewnienia i organizacji egzaminu końcowego potwierdzającego zdobytą wiedzę.
3.4	Wsparcie poszkoleniowe	Wykonawca jest zobowiązany zapewnić Zamawiającemu możliwość kontaktu z trenerem w celach merytorycznych przez okres co najmniej 14 dni po zakończeniu szkolenia.

5. Szkolenie nr 5 - Przeprowadzenie zaawansowanego szkolenia z zakresu administracji systemem Windows Server (zdalnie)

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne**	
1.1	Nazwa szkolenia	MS 55371 Administrowanie systemem Windows Server (lub szkolenie o równoważnym, autoryzowanym zakresie).
1.2	Forma	Szkolenie jest prowadzone na żywo, w formie zdalnej (online).
1.3	Czas trwania	Szkolenie musi obejmować minimum 5 dni, co stanowi łącznie co najmniej 40 godzin zajęć dydaktycznych.
1.4	Język	Szkolenie oraz wszystkie materiały muszą być w języku polskim.
1.5	Instruktor	Szkolenie musi być prowadzone przez Autoryzowanego Trenera Producenta (np. Microsoft Certified Trainer – MCT) lub trenera z równoważnymi, udokumentowanymi kwalifikacjami.
2.	**Zakres Merytoryczny**	
2.1	Administracja Wprowadzająca	Zakres szkolenia musi obejmować: Wprowadzenie do Windows Server.

2.2		Zakres szkolenia musi obejmować: Omówienie wersji Windows Server Core.
2.3		Zakres szkolenia musi obejmować: Przegląd zasad i narzędzi administrowania Windows Server.
2.4	Usługi Tożsamości (AD DS)	Zakres szkolenia musi obejmować: Przegląd usługi Active Directory Domain Services (AD DS).
2.5		Zakres szkolenia musi obejmować: Wdrażanie kontrolerów domeny.
2.6		Zakres szkolenia musi obejmować: Omówienie usługi Azure AD i integracji z AD DS.
2.7		Zakres szkolenia musi obejmować: Implementowanie Zasad Grupy (GPO).
2.8		Zakres szkolenia musi obejmować: Omówienie Active Directory Certificate Services.
2.9	Infrastruktura Sieciowa	Zakres szkolenia musi obejmować: Wdrażanie i zarządzanie usługami DHCP i DNS.
2.10		Zakres szkolenia musi obejmować: Wdrażanie i zarządzanie IPAM.
2.11		Zakres szkolenia musi obejmować: Konfigurację i wdrażanie dostępu zdalnego (VPN).
2.12		Zakres szkolenia musi obejmować: Wdrażanie Always On VPN.
2.13		Zakres szkolenia musi obejmować: Wdrażanie systemu NPS i Serwera WWW.
2.14	Pamięć Masowa i Pliki	Zakres szkolenia musi obejmować: Woluminy i systemy plików.
2.15		Zakres szkolenia musi obejmować: Implementowanie udostępniania plików.
2.16		Zakres szkolenia musi obejmować: Wdrażanie Storage Spaces.
2.17		Zakres szkolenia musi obejmować: Wdrażanie deduplikacji danych.
2.18		Zakres szkolenia musi obejmować: Wdrażanie iSCSI.
2.19		Zakres szkolenia musi obejmować: Wdrażanie rozproszonego systemu plików (DFS).
2.20	Wirtualizacja i Kontenery	Zakres szkolenia musi obejmować: Omówienie roli Hyper-V.
2.21		Zakres szkolenia musi obejmować: Konfigurowanie maszyn wirtualnych.
2.22		Zakres szkolenia musi obejmować: Zabezpieczanie wirtualizacji.
2.23		Zakres szkolenia musi obejmować: Omówienie konteneryzacji w Windows Server i platformy Kubernetes.
2.24	Wysoka Dostępność (HA)	Zakres szkolenia musi obejmować: Planowanie i tworzenie klastrów pracy awaryjnej (Failover Clustering).

2.25		Zakres szkolenia musi obejmować: Rozwiązania HA/DR z maszynami wirtualnymi Hyper-V.
2.26	Odzyskiwanie po Awarii (DR)	Zakres szkolenia musi obejmować: Wdrażanie Hyper-V Replica.
2.27		Zakres szkolenia musi obejmować: Wdrażanie Windows Server Backup.
2.28	Bezpieczeństwo	Zakres szkolenia musi obejmować: Ochrona poświadczeń i dostępu uprzywilejowanego.
2.29		Zakres szkolenia musi obejmować: Hardening Windows Server.
2.30		Zakres szkolenia musi obejmować: JEA (Just Enough Administration).
2.31		Zakres szkolenia musi obejmować: Zabezpieczanie i analizowanie ruchu SMB.
2.32		Zakres szkolenia musi obejmować: Zarządzanie aktualizacjami.
2.33	Monitoring	Zakres szkolenia musi obejmować: Wdrażanie natywnych narzędzi do monitorowania serwerów (Performance Monitor, Event Logs) i rozwiązywania problemów.
3.	**Materiały i Usługi w cenie**	
3.1	Egzamin	Wykonawca zobowiązany jest w ramach oferowanej ceny do zapewnienia, opłacenia i organizacji egzaminu końcowego potwierdzającego zdobytą wiedzę.
3.2	Materiały i Certyfikacja	Wykonawca dostarczy komplet oficjalnych, autoryzowanych materiałów szkoleniowych. Wykonawca zapewni imienne zaświadczenie o ukończeniu szkolenia.
3.3	Wsparcie poszkoleniowe	Wykonawca jest zobowiązany zapewnić Zamawiającemu możliwość kontaktu z trenerem w celach merytorycznych przez okres co najmniej 14 dni po zakończeniu szkolenia.

6. Szkolenie nr 6 - CCNA Cisco Certified Network Associate (zdalnie)

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne**	
1.1	Nazwa szkolenia	Cisco Certified Network Associate (CCNA) lub szkolenie o równoważnym, autoryzowanym zakresie.
1.2	Forma	Szkolenie jest prowadzone na żywo, w formie zdalnej (online).
1.3	Czas trwania	Szkolenie musi obejmować minimum 5 dni, co stanowi łącznie co najmniej 35 godzin zajęć dydaktycznych (Wymóg OPZ).
1.4	Język	Szkolenie oraz wszystkie materiały muszą być w języku polskim.
1.5	Instruktor	Szkolenie musi być prowadzone przez Autoryzowanego Trenera Producenta (np. Cisco Certified Systems Instructor – CCSI) lub trenera z równoważnymi, udokumentowanymi kwalifikacjami.

2.	**Zakres Merytoryczny**	
2.1	Podstawy Sieci (Rola)	Zakres szkolenia musi obejmować: Omówienie roli i komponentów sieci (urządzenia końcowe, pośredniczące).
2.2	Podstawy Sieci (Modele)	Zakres szkolenia musi obejmować: Modele odniesienia ISO/OSI i TCP/IP.
2.3	Adresacja (IPv4)	Zakres szkolenia musi obejmować: Adresacja IPv4 (klasy, podsieci, VLSM).
2.4	Adresacja (IPv6)	Zakres szkolenia musi obejmować: Adresacja IPv6 i mechanizmy przejścia.
2.5	Konfiguracja Podstawowa (IOS)	Zakres szkolenia musi obejmować: Omówienie systemu operacyjnego Cisco IOS.
2.6	Konfiguracja Podstawowa (Ustawienia)	Zakres szkolenia musi obejmować: Podstawowa konfiguracja urządzeń (nazwa, hasła, baner).
2.7	Zarządzanie Urządzeniami	Zakres szkolenia musi obejmować: Zarządzanie plikami konfiguracyjnymi i licencjami. Wykorzystanie protokołów do wykrywania urządzeń (CDP, LLDP).
2.8	Przełączanie (Switching)	Zakres szkolenia musi obejmować: Zasady działania przełączników warstwy 2 (tablica adresów MAC).
2.9	Wirtualne Sieci (VLAN)	Zakres szkolenia musi obejmować: Wprowadzenie i konfiguracja wirtualnych sieci lokalnych (VLAN).
2.10	Wirtualne Sieci (Trunking)	Zakres szkolenia musi obejmować: Konfiguracja łączy agregacyjnych (trunking 802.1Q). Konfiguracja routingu między sieciami VLAN (Inter-VLAN routing).
2.11	Routing (Statyczny)	Zakres szkolenia musi obejmować: Konfiguracja routingu statycznego dla protokołów IPv4 i IPv6.
2.12	Routing (Dynamiczny)	Zakres szkolenia musi obejmować: Wprowadzenie i podstawowa konfiguracja dynamicznego protokołu routingu OSPFv2 (implementacja single area).
2.13	Usługi IP (DHCP/NAT)	Zakres szkolenia musi obejmować: Konfiguracja serwera DHCP. Konfiguracja translacji adresów sieciowych (NAT).
2.14	Zarządzanie (Obsługa)	Zakres szkolenia musi obejmować: Konfiguracja usług sieciowych (NTP, Syslog). Wykorzystanie poleceń ping i traceroute do diagnostyki.
2.15	Bezpieczeństwo (ACL)	Zakres szkolenia musi obejmować: Omówienie zasad działania list kontroli dostępu (ACL). Konfiguracja ACL dla IPv4.
2.16	Bezpieczeństwo (Port Security)	Zakres szkolenia musi obejmować: Konfiguracja podstawowych mechanizmów bezpieczeństwa na przełącznikach (np. Port Security).
3.	**Materiały i Usługi w cenie**	
3.1	Egzamin	Wykonawca zobowiązany jest w ramach oferowanej ceny do zapewnienia, opłacenia i organizacji egzaminu końcowego potwierdzającego zdobytą wiedzę.
3.2	Materiały Autoryzowane	Wykonawca dostarczy komplet oficjalnych, autoryzowanych materiałów szkoleniowych.

3.3	Środowisko Laboratoryjne	Wykonawca musi zapewnić każdemu uczestnikowi indywidualny dostęp do zdalnego środowiska laboratoryjnego (wirtualnego lub fizycznego) na czas trwania szkolenia.
3.4	Certyfikat/Zaświadczenie	Wykonawca zapewni zaświadczenie o ukończeniu szkolenia.
3.5	Wsparcie poszkoleniowe	Wykonawca jest zobowiązany zapewnić Zamawiającemu możliwość kontaktu z trenerem w celach merytorycznych przez okres co najmniej 14 dni po zakończeniu szkolenia.

Część 2 – Cyberbezpieczeństwo dla pracowników i kadry zarządzającej

Przedmiotem tej części zamówienia jest dostarczenie i zapewnienie dostępu do platformy e-learningowej oferującej szkolenia z zakresu cyberbezpieczeństwa dla 69 **pracowników Zamawiającego**. Celem jest podniesienie świadomości i kompetencji pracowników w zakresie ochrony przed cyberzagrożeniami.

1. **Szkolenie nr 7 – Szkolenie elearningowe dla pracowników z testami socjotechnicznymi (zdalnie)**

Lp.	Kategoria	Parametr / Wymaganie
1.	**Wymagania Ogólne i Licencyjne**	
1.1	Przedmiot usługi	Dostarczenie platformy e-learningowej ze szkoleniami online z zakresu cyberbezpieczeństwa dla wszystkich pracowników Zamawiającego.
1.2	Liczba licencji	69 licencji dla pracowników.
1.3	Okres dostępu	Dostęp do platformy i szkoleń musi być zapewniony na okres do 31.05.2026 r.
1.4	Przedłużenie usługi	Musi istnieć możliwość zamówienia dostępu na nowy okres po zakończeniu świadczenia usługi.
2.	**Architektura i Dostępność Platformy**	
2.1	Dostępność	Platforma musi być dostępna zdalnie, przez całą dobę, 7 dni w tygodniu.
2.2	Dostęp z różnych urządzeń	Musi być zapewniony dostęp z dowolnego urządzenia z dostępem do Internetu.
3.	**Struktura i Jakość Treści Szkoleniowych**	
3.1	Struktura modułowa	Każde szkolenie musi być podzielone na co najmniej 4 moduły.
3.2	Zawartość modułu	Każdy moduł musi zawierać co najmniej: fabularny materiał wideo, materiał wideo z wyjaśnieniem zagadnień, tekstowy materiał merytoryczny oraz quiz wiedzy.
3.3	Jakość merytoryczna	Szkolenia muszą być przygotowane przez ekspertów w dziedzinie cyberbezpieczeństwa, a ich treść musi być aktualna i odnosić się do realnych zagrożeń.
4.	**Minimalny Zakres Merytoryczny Szkoleń**	
4.1	Ogólne Cyberbezpieczeństwo	Zakres tematyczny musi obejmować co najmniej: Socjotechnikę, tworzenie bezpiecznych haseł, bezpieczeństwo poczty e-mail, obronę przed phishingiem, weryfikację bezpieczeństwa stron WWW,

		bezpieczne korzystanie z przeglądarki, ataki smishing i vishing, zagrożenia dla urządzeń mobilnych i sieci Wi-Fi, zagrożenia w mediach społecznościowych, dobre praktyki korzystania z sieci.
5.	**Funkcjonalność Testów i Certyfikacji**	
5.1	Rodzaj pytań	Testy i quizy muszą składać się z pytań jednokrotnego i wielokrotnego wyboru.
5.2	Wymuszona kolejność	Platforma musi wymuszać sekwencyjne ukończenie modułów – brak możliwości podejścia do testu końcowego modułu przed ukończeniem materiałów wideo i tekstowych.
5.3	Warunek przejścia do kolejnego etapu	Pozytywne zaliczenie testu z danego modułu musi być warunkiem przejścia do kolejnego modułu.
5.4	Limit czasowy	Testy końcowe muszą mieć określony limit czasowy na ich ukończenie.
5.5	Certyfikat ukończenia	Ukończenie całego kursu i zaliczenie testu końcowego muszą skutkować automatycznym wygenerowaniem imiennego certyfikatu dla użytkownika.
6.	**Zarządzanie Użytkownikami**	
6.1	Role użytkowników	Platforma musi wspierać co najmniej dwie role: administrator i użytkownik.
6.2	Dane użytkownika	Wymagane dane użytkownika to minimum: Imię, nazwisko i unikalny w obrębie organizacji adres e-mail.
6.3	Proces rejestracji	Po dodaniu użytkownika do platformy, musi on otrzymać automatyczną wiadomość e-mail z zaproszeniem i linkiem do ustawienia pierwszego hasła.
6.4	Funkcje administratora	Administrator musi mieć możliwość: edycji danych użytkowników, aktywacji/dezaktywacji kont oraz usuwania kont nieaktywnych.
6.5	Raportowanie postępów	Administrator musi mieć wgląd w postępy nauki i wyniki testów w całej organizacji oraz dla poszczególnych grup.
7.	**Funkcje Dodatkowe**	
7.1	Powiadomienia	Platforma musi posiadać funkcję wysyłania do użytkowników automatycznych przypomnień (newsletter) o nieukończonych modułach szkoleniowych.
7.2	Możliwość rozszerzenia	Platforma musi umożliwiać rozszerzenie subskrypcji o inne moduły szkoleniowe z oferty Wykonawcy.
Testy socjotechniczne		
8	**Spotkanie Ustalające**	Wymagane jest spotkanie z Zamawiającym, na którym muszą zostać ustalone cele testu.
8.1		Należy pozyskać informacje niezbędne do przygotowania kampanii.
8.2		Konieczne jest ustalenie preferencji Zamawiającego dotyczących scenariuszy.
9	**Opracowanie Scenariusza**	Wykonawca musi opracować i przedłożyć propozycję scenariusza kampanii na podstawie ustaleń ze spotkania.
9.1		Oferta musi umożliwiać Klientowi wybór spośród dostępnych wariantów scenariuszy (przykładowo: "Kampania wewnętrzna - tanie

		telefony", "Vouchery okolicznościowe", "Nowy pracownik działu IT", "Przydzielenie premii", "Wyrównanie płac na podobnym stanowisku").
10	**Akceptacja**	Wymagane jest pisemne zatwierdzenie ostatecznej wersji scenariusza przez Zamawiającego przed rozpoczęciem kampanii.
11	**Realizacja Techniczna**	Kampania musi być zrealizowana z wykorzystaniem jednej dedykowanej domeny.
11.1		Domena ta musi być wykupiona wyłącznie na potrzeby przeprowadzenia testu.
11.2		Wysyłka spreparowanego e-maila musi nastąpić do listy adresatów wskazanej przez Zamawiającego.
12	**Monitoring Działań**	W trakcie kampanii obowiązkowe jest monitorowanie następujących interakcji: otwarcia wiadomości e-mail.
12.1		Monitorowanie kliknięcia w link zawarty w wiadomości.
12.2		Monitorowanie próby podania poświadczeń (jeśli scenariusz kampanii to przewiduje).
13	**Raportowanie**	Po zakończeniu testu Wykonawca musi sporządzić szczegółowy raport z przebiegu kampanii.
13.1		Raport ten musi zawierać opis uzyskanych rezultatów i wnioski.
14	**Wymogi Organizacyjne**	Poufność: Zamawiający zobowiązuje się do zachowania pełnej poufności co do planowanej kampanii.

2. **Szkolenie nr 8 – Bezpieczeństwo informacji dla pracowników i kadry zarządzającej (stacjonarne)**

Przedmiotem tej części zamówienia jest usługa przeprowadzenia szkolenia **dla 69 pracowników Zamawiającego** z zakresu strategii bezpieczeństwa dla pracowników i kadry kierowniczej. Celem szkolenia jest doskonalenie umiejętności decyzyjnych w zakresie zarządzania ryzykiem cybernetycznym oraz zapoznanie z realnymi zagrożeniami i skutecznymi strategiami obronnymi.

Lp.	Kategoria	Wymagania Szczegółowe do OPZ
I. WYMAGANIA ORGANIZACYJNE I OGÓLNE (Wspólne)		
1.	**Język Usług**	Szkolenia oraz wszystkie materiały muszą być prowadzone i dostarczone w języku polskim.
2.	**Instruktor**	Szkolenia muszą być prowadzone przez trenera z praktycznym doświadczeniem w obszarze cyberbezpieczeństwa.
3.	**Certyfikacja**	Uczestnicy muszą otrzymać zaświadczenie ukończenia szkolenia.
4.	**Wsparcie Porealizacyjne**	Wykonawca musi zapewnić 14-dniowy kontakt mailowy z trenerem w celach merytorycznych po zakończeniu szkolenia.
5.	**Materiały**	Wykonawca dostarczy Zamawiającemu komplet materiałów dydaktycznych w formie elektronicznej lub papierowej.
6.	**Zgodność**	Kurs dla pracowników biurowych jest zgodny z dyrektywą NIS2 i pomaga spełnić najnowsze wymogi dotyczące bezpieczeństwa sieci i informacji.

7.	**Termin Realizacji**	Szkolenie dla kadry kierowniczej musi zostać zrealizowane nie później niż do 31.05.2026 r.
II. O7RGANIZACJA DNIA SZKOLENIOWEGO		
8.	**Format Dnia**	Szkolenia muszą trwać łącznie minimum 6 godzin dydaktycznych w ciągu jednego dnia.
9.		Dzień musi być zorganizowany w formule dwóch bloków szkoleniowych.
10.	**Liczba Grup**	W ciągu jednego dnia szkoleniowego Wykonawca musi przeszkolić 2 grupy.
11.	**Uczestnicy**	Szkolenie jest skierowane do każdego pracownika w firmie bez względu na jego wiedzę i umiejętności informatyczne.
12.	**Uczestnicy (Kierownictwo)**	Ilość uczestników szkolenia dla kadry kierowniczej to 6 osób.
13.	**Lokalizacja**	Szkolenie dla pracowników musi być przeprowadzone w siedzibie Zamawiającego.
14.	**Forma (Kierownictwo)**	Szkolenie dla kadry kierowniczej musi być przeprowadzone w siedzibie Zamawiającego.
III. PROGRAM SZKOLENIA: KADRA KIEROWNICZA (min. 3h)		
15.	**Wprowadzenie i Cel**	Szkolenie ma na celu podniesienie świadomości z zagrożeń cyberbezpieczeństwa kadry kierowniczej.
16.	**Ataki i Ryzyka**	Przykłady phishingu.
17.		Zagrożenia typu Zero-day exploit.
18.		Inne metody dostarczania złośliwego oprogramowania.
19.	**Ochrona i Strategia**	Rola sztucznej inteligencji w cyberatakach i obronie.
20.		Bezpieczeństwo haseł.
21.		Ryzyka związane z używaniem sprzętu prywatnego do celów służbowych.
22.		Metody zwiększania odporności na cyberataki.
23.	**Zarządzanie**	OPSEC (Bezpieczeństwo operacyjne) w praktyce.
24.	**Podsumowanie**	Sesja pytań i odpowiedzi.
IV. PROGRAM SZKOLENIA: PRACOWNICY BIUROWI (3h)		
25.	**Wprowadzenie i Zagrożenia**	Wprowadzenie do cyberprzestępczości i podstawy cyberbezpieczeństwa.
26.		Zorganizowane grupy cyberprzestępcze (jak działają i dlaczego są groźne).
27.		Korzyści dla cyberprzestępców: Co zyskują atakując Twoje dane.
28.		Straty dla firmy: Skutki udanego cyberataku.
29.	**Rodzaje Ataków**	Al w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji.
30.		Ataki DoS/DDoS i Ataki 0-day.
31.		Rodzaje ataków na pracowników biurowych.

32.	**Socjotechnika i Mail**	Ataki socjotechniczne, czyli niewinne wyłudzanie danych.
33.		Phishing jako metoda okradania naszych kont bankowych.
34.		Spam jako niegroźny sposób na groźne ataki.
35.	**Bezpieczeństwo Fizyczne/Danych**	Bezpieczeństwo haseł i skanowanie kart płatniczych.
36.		Bezpieczne przekazywanie haseł współpracownikom i kradzież tożsamości.
37.		Fizyczne bezpieczeństwo: Jak zabezpieczyć miejsce pracy.
38.	**Zagrożenia Zewnętrzne**	Opłacona faktura jako sposób przemycenia wirusa do naszego systemu.
29.		Znaleziony pendrive, jako pozwolenie na atak cyberprzestępcy.
40.		Sprzęt prywatny vs. firmowy: Jak zarządzać bezpieczeństwem urządzeń.
41.	**Metody Obrony**	Skuteczne metody ochrony i zwiększenie odporności na cyberataki.

Część 3 – Szkolenie specjalistyczne dla Informatyków z zakresu wdrażanych rozwiązań technicznych

Przedmiotem tej części zamówienia jest usługa przeprowadzenia szkolenia **dla 2 (dwóch) pracowników Zamawiającego** z zakresu **konfiguracja urządzeń UTM**.

1. **Szkolenie nr 9 – Zapora sieciowa & Podstawy Bezpieczeństwa Sieci (stacjonarne)**

Lp.	Kategoria	Wymagania
1	**Nazwa i Cel**	Celem szkolenia jest konfiguracja i administracja rozwiązaniami klasy UTM WatchGuard.
2	**Czas i Forma**	Minimum 4 dni.
3		Każdy dzień szkolenia musi obejmować minimum 7 godzin zajęć.
4		Szkolenie musi być prowadzone przez certyfikowanych inżynierów.
5		Prowadzący muszą mieć doświadczenie we wdrożeniach w złożonych środowiskach u klientów.
6	**Certyfikacja**	Cena musi obejmować imienny Certyfikat ukończenia szkolenia od autoryzowanego partnera szkoleniowego WatchGuard.
7	**Materiały**	Uczestnicy muszą otrzymać darmowe materiały szkoleniowe.
8		Wymaganym materiałem jest Przewodnik "Fireware Essentials Student Guide".
9	**Zakres - Administracja**	Konfiguracja i zarządzanie Firebox (w tym otwieranie i zapisywanie plików konfiguracyjnych, zdalna administracja).
10		Dodawanie kluczy licencyjnych.
11		Backup i przywracanie konfiguracji urządzenia.
12		Aktualizacja systemu operacyjnego Fireware.

13	**Zakres - Zagrożenia**	Domyślna ochrona przed zagrożeniami.
14		Blokowanie adresów IP i portów używanych przez hackerów.
15		Automatyczne blokowanie adresów IP, które generują podejrzany ruch.
16	**Zakres - Logowanie**	Logowanie i wysyłanie powiadomień.
17		Monitorowanie za pomocą Firebox System Manager i Fireware Web UI.
18		Użycie WatchGuard Dimension do wyszukiwania logów i generowania raportów.
19	**Zakres - Sieć**	Konfigurowanie zewnętrznych interfejsów sieciowych (statyczny IP, DHCP, PPPOE).
20		Konfigurowanie zaufanych i opcjonalnych interfejsów sieciowych.
21		Używanie Fireboxa jako serwera DHCP.
22		Obsługa podsieci w ramach jednego interfejsu (Secondary network).
23		Ustawianie i działanie sieci VLAN.
24		Konfiguracja Multi-WAN (przełączanie awaryjne i przepełnienie interfejsu).
25		Konfiguracja SD-WAN i Static Routing.
26	**Zakres - NAT**	Dynamic NAT co to jest i jak skonfigurować.
27		Static NAT do ochrony serwerów i NAT 1-do-1.
28	**Zakres - Zapora**	Podstawy zasad zapory i różnice między filtrem pakietów a polityką proxy.
29		Tworzenie niestandardowego pakietu filtrów i poprawna kolejność reguł.
30		Blokowanie połączeń z wybranych krajów z wykorzystaniem geolokalizacji.
31	**Zakres - Proxy**	Konfigurowanie proxy DNS, aby chronić serwer DNS.
32		Konfiguracja WebBlocker oraz zasady HTTP-proxy i HTTPS-proxy.
33		E-mail Proxy i blokowanie spamu (Aktywacja i konfiguracja Spam Blocker'a).
34		Zapobieganie utracie danych i APT Blocker.
35	**Zakres - Moduły**	Instalacja i konfigurowanie Gateway AntiVirus.
36		Instalacja i konfigurowanie Data Loss Prevention.
37		Instalacja i konfigurowanie Intrusion Prevention Service (IPS).
38		Instalacja i konfigurowanie Application Control i Botnet Detection.
39	**Zakres - Autoryzacja**	Uwierzytelnianie (jak działa z Firebox'em, jakie typy można zastosować).
40		Używanie Fireboxa do uwierzytelnienia użytkowników i grup.
41	**Zakres - VPN**	Konfiguracja Mobilny VPN z IKEv2, SSL, L2TP, IPSec.
42		Konfiguracja Branch Office VPN (BOVPN) (w tym ręczna konfiguracja i rozwiązywanie problemów).

VII. Warunki udziału w postępowaniu.

1. Wykonawca ubiegający się o realizację Części 1, 2 musi spełniać następujące warunki:

1) Wykonawca musi wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, zrealizował z należytą starannością co najmniej 3 usługi polegające na przeprowadzeniu specjalistycznych szkoleń z zakresu cyberbezpieczeństwa. Łączny czas trwania każdej z tych 3 wykazanych usług musiał wynosić minimum 7 dni dydaktycznych (tj. min. 49 godzin dydaktycznych).

2) Wykonawca musi posiadać status instytucji szkoleniowej, potwierdzony aktualnym Wpisem do Rejestru Instytucji Szkoleniowych.

3) Wykonawca musi wykazać, że wdrożył i utrzymuje system zarządzania jakością zgodny z normą PN-EN ISO 9001:2015-10 w zakresie świadczenia usług szkoleniowych, co musi być potwierdzone ważnym certyfikatem.

4) Wykonawca musi posiadać status autoryzowanego ośrodka szkoleniowego EC-COUNCIL i Microsoft lub równoważny status w zakresie realizacji szkolenia/szkoleń objętych ofertą.

5) Wykonawca musi wykazać, że osoby odpowiedzialne za merytoryczne prowadzenie szkoleń posiadają stosowną wiedzę potwierdzoną ważnymi certyfikatami w zakresie objętym przedmiotem zamówienia.

2. Wykonawca ubiegający się o realizację Części 3 musi spełniać następujące warunki:

1) Wykonawca musi wykazać, że posiada autoryzację firmy Watchguard lub równoważny status na świadczenie usług polegających na oferowaniu i sprzedaży szkoleń z zakresu technologii Watchguard

3. Przesłanie oferty w odpowiedzi na niniejsze Zapytanie ofertowe jest jednoznaczne ze złożeniem oświadczenia, że Wykonawca spełnia powyższe kryteria.

4. Złożenie oferty jest jednoznaczne z zapoznaniem się z treścią zapytania ofertowego i akceptacją warunków realizacji zamówienia określonych w niniejszym Zapytaniu Ofertowym.

5. Zamawiający informuje, że niniejsze zapytanie ofertowe nie stanowi oferty zawarcia umowy, ani też oferty prowadzenia negocjacji w tym celu i jest skierowane do wielu adresatów.

VIII. Dokumenty i Oświadczenia Składane Wraz z Ofertą w Celu Potwierdzenia Spełnienia Warunków Udziału

Wykonawca, wraz z ofertą, zobowiązany jest złożyć następujące dokumenty w celu udokumentowania spełnienia warunków określonych w sekcji VII (Warunki udziału w postępowaniu):

1. Oświadczenie Wykonawcy (Załącznik nr 2):
    - Wypełniony i podpisany Załącznik nr 2 stanowiący oświadczenie Wykonawcy o spełnieniu wszystkich warunków udziału w postępowaniu.
2. Doświadczenie Wykonawcy (Załącznik nr 2b):

- Wykaz zrealizowanych usług, potwierdzający zrealizowanie w okresie ostatnich 3 lat przed upływem terminu składania ofert, co najmniej 3 usług spełniających warunki określone w rozdział 7 punkt 1 podpunkt 1

3. Status Instytucji Szkoleniowej:

   - Aktualna kopia (np. wydruk) Wpisu do Rejestru Instytucji Szkoleniowych (RIS), potwierdzająca status Wykonawcy jako instytucji szkoleniowej.

4. Certyfikat Jakości:

   - Kopia ważnego certyfikatu potwierdzającego wdrożenie i utrzymanie Systemu Zarządzania Jakością zgodnego z normą PN-EN ISO 9001:2015-10 w zakresie świadczenia usług szkoleniowych.

5. Kwalifikacje Kadry Technicznej:

   - Kopia ważnego certyfikatu osoby(osób) bezpośrednio prowadzącej(ych) szkolenia, potwierdzająca(e) jej(ich) stosowną wiedzę i kwalifikacje w zakresie objętym przedmiotem zamówienia

6. Autoryzacja Produktowa:

   - Dokument potwierdzający autoryzację firmy Watchguard lub równoważny status na świadczenie szkoleń w zakresie technologii Watchguard.

IX. Wymagania dotyczące Formy i Sposobu Składania Ofert oraz Komunikacji

1. Informacje ogólne

1) Wykonawcy zobowiązani są zapoznać się dokładnie z informacjami zawartymi w niniejszym Zapytaniu Ofertowym (ZO) i przygotować ofertę zgodnie z wymaganiami określonymi w tym dokumencie, a w szczególności by treść oferty odpowiadała treści ZO.

2) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

3) Oferty zaleca się sporządzić pismem maszynowym lub komputerowym.

4) Oferty zaleca się sporządzić na załączonym formularzu (Załącznik nr 1 – Formularz ofertowo-cenowy). Dopuszcza się sporządzenie własnych formularzy z zastrzeżeniem dokonywania jakichkolwiek zmian merytorycznych w stosunku do wzorów.

2. Sposób i forma składania oferty

1) Oferty w postępowaniu można składać wyłącznie z wykorzystaniem platformy e-Doręczeń na adres: AE:PL-67264-75623-FBDDU-15

2) Ofertę składa się, pod rygorem nieważności, w formie elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym lub podpisem kwalifikowanym.

3) Zamawiający odrzuci oferty, które nie zostały podpisane w sposób określony w pkt. 2, w szczególności odrzuci oferty podpisane odręcznie i zeskanowane.

4) Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z formą reprezentacji określoną w rejestrze (np. KRS) lub przez osobę umocowaną, przy czym pełnomocnictwo musi być załączone do oferty.

5) Oferty zaleca się złożyć w formacie PDF. Zaleca się, aby oferta wraz z załącznikami miała formę pojedynczego pliku PDF lub spakowanego archiwum np. ZIP, RAR, itp.

6) Za datę złożenia oferty uważa się datę i godzinę wpłynięcia oferty na platformę e-Doręczeń.

7) Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

8) Zamawiający nie dopuszcza składania ofert wariantowych. Złożenie przez Wykonawcę więcej niż jednej oferty na zamówienie i/lub oferty wariantowej spowoduje odrzucenie przez Zamawiającego wszystkich złożonych ofert.

3. Wymogi Cenowe i Waluta

1) Oferty należy złożyć z ceną wyrażoną w Polskich Złotych (PLN). Oferty złożone z ceną wyrażoną w innej walucie zostaną odrzucone.

2) W przypadku, gdy złożone przez wykonawców dokumenty, oświadczenia dotyczące warunków udziału w postępowaniu zawierają dane / informacje w innych walutach niż PLN (złoty polski), Zamawiający jako kurs przeliczeniowy waluty przyjmie kurs NBP z dnia publikacji ogłoszenia. Jeżeli w dniu ogłoszenia nie będzie opublikowany średni kurs walut przez NBP, Zamawiający przyjmie kurs przeliczeniowy z ostatniej opublikowanej tabeli kursów NBP przed dniem publikacji ogłoszenia o zamówieniu.

4. Komunikacja z Zamawiającym

1) Komunikacja w postępowaniu (w tym ogłoszenie ZO, składanie ofert, przekazywanie dokumentów i oświadczeń) odbywa się drogą elektroniczną za pomocą platformy e-Doręczeń na adres: **AE:PL-67264-75623-FBDDU-15**. Dopuszcza się przesyłanie pytań dotyczących treści ZO za pośrednictwem poczty elektronicznej na zasadach określonych w pkt 4.2).

2) Wnioski o wyjaśnienie treści Zapytania Ofertowego należy składać za pośrednictwem platformy e-Doręczeń (kanał podstawowy) lub na adres e-mail: **informatyk@gmina.swidnica.pl** (kanał pomocniczy). Za datę i godzinę wpływu zapytania uznaje się moment jego zarejestrowania na platformie e-Doręczeń lub – w przypadku wiadomości e-mail – czas wpłynięcia na serwer pocztowy Zamawiającego.

3) Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 3 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie wpłynął do Zamawiającego (zgodnie z zasadami określonymi w pkt 4.2) nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. W przypadku wpływu wniosku po tym terminie, Zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpoznania.

4) Treść zapytań wraz z wyjaśnieniami Zamawiający opublikuje wyłącznie na stronie internetowej prowadzonego postępowania.

5) Osobami uprawnionymi do kontaktowania się z wykonawcami są:

- Ireneusz Filiacz – informatyk, tel. 748523067 wew. 305. e-Mail: i.filiacz@gmina.swidnica.pl;
- Daniel Grzybowski – informatyk, tel. 748523067 wew. 305. e-Mail: informatyk@gmina.swidnica.pl

5. Termin związania ofertą

1) Termin związania ofertą wynosi 30 dni i rozpoczyna się wraz z upływem terminu składania ofert.

2) Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.

3) Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 30 dni.

4) Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie skutkuje negatywnymi konsekwencjami prawnymi w niniejszym postępowaniu.

6. Wyłączenia z postępowania Wyłączenie z uwagi na powiązania (osobowe/kapitałowe):

a) O udzielenie zamówienia nie mogą ubiegać się Wykonawcy powiązani z Zamawiającym i/lub osobami biorącymi udział w przygotowaniu lub prowadzeniu postępowania o udzielenie zamówienia.

b) Przez powiązania osobowe lub kapitałowe rozumie się powiązania polegające na: a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej; b) posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa); c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika; d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z Zamawiającym lub osobami prowadzącymi postępowanie; e) pozostawaniu z Zamawiającym w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

7. Wyłączenie związane z sankcjami (agresja na Ukrainę):

1) Zamówienie nie może zostać udzielone podmiotom, wobec których zachodzi jakakolwiek z okoliczności wskazanych w art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
2) Zamawiający informuje, że wykluczeniu z postępowania na podstawie pkt 13.2 ZO podlegają:

a) wykonawcy wymienieni w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia

17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 powołanej ustawy;

b) wykonawcy, których beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t. j. Dz. U. z 2023 r., poz. 1124 ze zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile zostali wpisani na ww. listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego;

c) wykonawcy, których jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (t. j. Dz. U. z 2023 r. poz. 120 ze zm.) jest podmiot wymieniony w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisany na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

3) Zamówienie nie może zostać udzielone podmiotom, wobec których zachodzi jakakolwiek z okoliczności wskazanych w art. 7 ustawy z dnia 13 kwietnia 2022 r. oraz w art. 5k Rozporządzenia Rady (UE) nr 833/2014. Wykluczeniu podlegają w szczególności Wykonawcy wpisani na listy sankcyjne lub kontrolowani przez podmioty objęte sankcjami.

X. Termin wykonania zamówienia i warunki płatności

1. Wykonawca wykona przedmiot zamówienia w terminie do 31.05.2026 roku od dnia zawarcia Umowy. Terminy wykonania szkoleń zostaną ustalone po wybraniu Wykonawcy lub Wykonawców. Terminy wykonania poszczególnych szkoleń powinny być ustalone w taki sposób, aby dla tych samych grup pracowników nie nakładały się na siebie.

2. Zapłata za wykonany przedmiot zamówienia nastąpi po prawidłowym wykonaniu przedmiotu zamówienia, na podstawie faktury VAT wystawionej przez Wykonawcę, w terminie 14 dni od dnia jej doręczenia Zamawiającemu, z zastrzeżeniem ust. 3 poniżej.

3. Zapłata za wykonany przedmiot zamówienia będzie następowała w częściach, po każdym odebranym szkoleniu potwierdzonym Protokołem odbioru częściowego, stanowiącym Załącznik nr 4 do Zapytania Ofertowego, stwierdzającym kompletność i zgodność wykonania przedmiotu zamówienia oraz poprawnie wystawiona faktura VAT. Podstawą do wystawienia przez Wykonawcę faktury VAT za dane szkolenie będzie podpisany bez uwag Protokół odbioru częściowego. Wartość faktury będzie odpowiadać pełnej wartości danego szkolenia, określonej w formularzu ofertowym Wykonawcy, stanowiącemu płatność etapową.

4. Dane do faktury:

   NABYWCA:
   Gmina Świdnica
   ul. B. Głowackiego 4,
   58-100 Świdnica
   NIP: 8842365226, REGON: 890718389
   ODBIORCA:
   Urząd Gminy Świdnica
   ul. B. Głowackiego 4,
   58-100 Świdnica

XI. Kryteria wyboru najkorzystniejszej oferty

1. Zamówienie zostało podzielone na 3 (trzy) odrębne części. Zamawiający dopuszcza możliwość składania ofert częściowych. Wykonawca może złożyć ofertę na jedną, kilka lub wszystkie części zamówienia.

2. Zamawiający podczas wyboru najkorzystniejszej oferty będzie kierował się kryterium 100% cena dla poszczególnych części, zgodnie z Załącznikiem nr 1.

3. W przypadku braku możliwości wyboru z uwagi na identyczną cenę, Zamawiający wybierze ofertę, której Oferent zaoferuje:

   Najwyższą łączną liczbę certyfikatów instruktorskich/trenerskich lub uznanych certyfikatów branżowych, posiadanych przez osoby dedykowane do realizacji danej Części Zamówienia.

XII. Klauzula informacyjna RODO

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

1) **Administratorzy Danych Osobowych:** Administratorami Państwa danych osobowych w związku z niniejszym postępowaniem są:
   a) **Gmina Świdnica (jako Zamawiający),** ul. B. Głowackiego 4, 58-100 Świdnica, e-mail: urząd@gmina.swidnica.pl, tel. 74 8523067.
   b) **Minister Funduszy i Polityki Regionalnej (MFiPR)** – Instytucja Zarządzająca (IZ), ul. Wspólna 2/4, 00-926 Warszawa.
   c) **Centrum Projektów Polska Cyfrowa (CPPC) –** Instytucja Pośrednicząca (IP) i Beneficjent FERC, ul. Spokojna 13A, 01-044 Warszawa.

2) **Inspektor Ochrony Danych (IOD Gminy Świdnica):** Gmina Świdnica wyznaczyła Inspektora Ochrony Danych, którym jest Pan Krzysztof Olejniczak. Kontakt z IOD jest możliwy pod adresem e-mail: krzysztof.olejniczak@comars.pl lub telefonicznie: 609 010 402.

3) **Cel i Podstawa Przetwarzania:** Państwa dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia niniejszego postępowania zgodnie z Regułami Konkurencyjności oraz w celu zawarcia i realizacji umowy.

4) **Okres Przechowywania Danych:** Dane osobowe będą przechowywane przez okres 2 lat od dnia zakończenia postępowania, a jeżeli czas trwania umowy przekracza 2 lata, okres przechowywania obejmuje cały czas trwania umowy. Okres ten wynika z wymogów archiwizacji dokumentacji projektowej finansowanej ze środków Unii Europejskiej (FERC).

5) **Prawa osób, których dane dotyczą:** Przysługuje Państwu prawo do: dostępu do swoich danych, sprostowania/uzupełnienia, żądania ograniczenia przetwarzania danych, wniesienia sprzeciwu, oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

6) **Obowiązek podania danych:** Obowiązek podania przez Państwa danych osobowych jest niezbędny do wzięcia udziału w postępowaniu i zawarcia umowy. Konsekwencje niepodania określonych danych wynikają z warunków niniejszego Zapytania Ofertowego.

7) **Zautomatyzowane Decyzje:** W odniesieniu do Państwa danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.

2. Pełna Klauzula FERC: Szczegółowe zasady i ograniczenia dotyczące przetwarzania danych przez Administratorów Projektowych (MFiPR i CPPC), w tym o pozostałych celach, podstawach prawnych, odbiorcach oraz ograniczeniach praw Wykonawców, zawarte są w Załączniku nr 5 - Klauzula informacyjna FERC.

8. Lista załączników

1. Załącznik nr 1 - Formularz ofertowo-cenowy
2. Załącznik nr 2 - Oświadczenie
3. Załącznik nr 3 - Wzór Umowy
4. Załącznik nr 4 - Protokół odbioru częściowego
5. Załącznik nr 4a - Protokół odbioru końcowego
6. Załącznik nr 5 – Klauzula informacyjna FERC