

Miasto i Gmina Sztum

Referat Organizacyjny i Zamówień Publicznych
ul. Mickiewicza 39, 82 – 400 Sztum
NIP 579-22-11-352, REGON 170747773
tel. (55) 640 63 01/02, (55) 640 63 03

Sztum, dnia 22.01.2026.

ZAPYTANIE OFERTOWE

*w postępowaniu o udzielenie zamówienia
o wartości nie przekraczającej równowartości 170 000 złotych netto*

Postępowanie prowadzone jest bez stosowania przepisów ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych, na podstawie Regulaminu wewnętrznego.

Miasto i Gmina Sztum
ul. Mickiewicza 39
82-400 Sztum

zaprasza do złożenia oferty na:

Przeprowadzenie szkoleń w ramach projektu Cyberbezpieczny Samorząd z podziałem na części.

Część 1: Szkolenie dla administratora systemu monitorującego infrastrukturę IT (Axence nVision).

Część 2: Szkolenie techniczne z zakresu ochrony styku sieci firmowej z Internetem (UTM Stormshield).

Część 3: Administrowanie systemem Windows Server

Część 4: Szkolenie przeznaczone dla administratora Active Directory w Microsoft Windows Server 2019/2022.

I. Opis przedmiotu zamówienia:

1. Termin i Miejsce Realizacji:

- 1) Wszystkie szkolenia muszą zostać zrealizowane w terminie do dnia **30 kwietnia 2026 r.** Konkretnie daty zostaną ustalone z Wykonawcą po podpisaniu umowy, jednak nie później niż 7 dni przed planowanym rozpoczęciem szkoleń.
- 2) Szkolenia muszą odbyć się w formie **stacjonarnej**. Zamawiający dopuszcza realizację szkolenia w dowolnej lokalizacji na terenie kraju.
- 3) Zamawiający dopuszcza realizację szkolenia zarówno w formie indywidualnej (tylko dla pracownika Zamawiającego), jak i w grupach otwartych.

- 4) Po zakończeniu szkolenia Wykonawca wystawi imienne świadectwo lub certyfikat potwierdzający ukończenie kursu, zawierający zakres tematyczny szkolenia oraz liczbę godzin.

Część 1:

Szkolenie dla administratora systemu monitorującego infrastrukturę IT (Axence nVision)

Przedmiotem zamówienia jest udział przedstawiciela Zamawiającego w dwudniowym, certyfikowanym szkoleniu stacjonarnym (2 x 8h) dotyczącym zaawansowanej administracji systemem do monitorowania infrastruktury IT.

- Szkolenie powinno mieć charakter warsztatów eksperckich, prowadzonych przez osobę posiadającą doświadczenie praktyczne oraz kompetencje szkoleniowe w zakresie administrowania systemami monitorującymi infrastrukturę IT. Program szkolenia powinien obejmować przekazanie uczestnikom pogłębionej wiedzy praktycznej, niezbędnej do skutecznego i efektywnego zarządzania systemem w środowisku produkcyjnym.
Zakres szkolenia administracyjnego Axence nVision: uruchomienie, konfiguracja, utrzymanie.
- Wprowadzenie do platformy: architektura, role, licencjonowanie, model wdrożenia w środowisku lokalnym i domenowym; najczęstsze scenariusze użycia w IT.
- Przygotowanie środowiska i instalacja: wymagania serwera, baza danych, konfiguracja usług, aktualizacje; podstawowe utwardzenie i dobre praktyki eksploatacyjne.
- Onboarding urządzeń: metody wdrożenia agentów, grupowanie i tagowanie; podstawowa diagnostyka połączeń i kompletności danych.
- Monitoring i sieć: konfiguracja skanowania i odkrywania zasobów; mapy i zależności; alertowanie i progi, reakcje na zdarzenia; szybki przegląd danych z urządzeń końcowych.
- Inwentaryzacja i zgodność: inwentaryzacja sprzętu oraz oprogramowania; audyty licencyjne; ewidencja i raportowanie środków trwałych, przygotowanie danych pod kontrolę i sprawozdawczość.
- Użytkownicy i polityki: zarządzanie kontami lokalnymi oraz domenowymi; role i uprawnienia; polityki bezpieczeństwa oraz analiza aktywności w ujęciu administracyjnym.
- Ochrona danych i nośników: polityki kontroli urządzeń zewnętrznych; przypisywanie uprawnień; monitoring operacji na plikach; alarmy i scenariusze reagowania.
- HelpDesk i proces obsługi: konfiguracja kanałów zgłoszeń; klasyfikacja, priorytety, SLA; delegowanie i zastępstwa, plan nieobecności; narzędzia wsparcia zdalnego i „live help”.
- SmartTime i perspektywa menedżerska: metryki aktywności, klasyfikacja aplikacji; role menedżerskie i zakres dostępu; interpretacja danych i typowe nadużycia; widok użytkownika i komunikacja zasad.
- Raportowanie i operacje utrzymaniowe: dashboardy i raporty cykliczne; harmonogramy zadań; kopie konfiguracji i odtwarzanie; typowe problemy i checklista uruchomienia produkcyjnego.

Część 2:**Szkolenie techniczne z zakresu ochrony styku sieci firmowej z Internetem (UTM Stormshield)**

Administrowanie urządzeniem klasy UTM – Stormshield - min. 21 h w podziale na 3 dni robocze

Firma szkoleniowa powinna być autoryzowanym ośrodkiem szkoleniowym szkoleniowym firmy Stormshield w Polsce.

Minimalne wymagania dotyczące szkolenia:

- Program szkolenia i certyfikacje
- Rozpoczęcie pracy z urządzeniem
- Rejestracja w strefie klienta i dostęp zasobów
- Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
- Ustawienia systemowe i uprawnienia administratorów
- Instalacja licencji i aktualizacja systemu
- Tworzenie kopii zapasowej i przywracanie konfiguracji
- Zbieranie logów i monitorowanie
- Przedstawienie kategorii zbieranych logów
- 10. Wykresy historyczne i monitorowanie
- Obiekty
- Typy obiektów oraz ich wykorzystanie
- Obiekty sieciowe i obiekt typu „router”
- Konfiguracja sieci
- Tryby pracy urządzenia
- Typy interfejsów
- Typy routingu oraz ich priorytety
- Translacja adresów sieciowych (NAT)
- Translacja połączeń wychodzących (maskarada)
- Translacja połączeń przychodzących (przekierowanie)
- Translacja dwukierunkowa (jeden do jeden)
- Filtrowanie ruchu sieciowego (Firewall)
- Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)13.
- Szczegółowy opis parametrów reguły Firewall
- Kolejność przetwarzania reguł Firewall i NAT
- Ochrona aplikacji
- Implementacja filtrowania URL dla ruchu http i https
- Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
- Moduł IPS i stosowanie profili inspekcji
- Użytkownicy i uwierzytelnianie
- Konfiguracja usługi katalogowej
- Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL,
- SPNEGO, SSO)
- Rejestracja użytkowników
- Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania

- Wirtualne sieci prywatne (VPN)
- Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
- Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
- Tunele VTI
- SSL VPN
- Zasada działania
- Konfiguracja

Część 3:

Administrowanie systemem Windows Server

Przedmiotem zamówienia jest realizacja pięciodniowego szkolenia 5 d x 8 h lekcyjnych (razem: 40 h lekcyjnych - jedna godzina lekcyjna to 45 minut) technicznego, obejmującego zagadnienia związane z administracją systemem serwerowym wykorzystywanym do zarządzania tożsamością, siecią, pamięcią masową oraz zasobami obliczeniowymi w środowiskach informatycznych.

Moduł 1: Wprowadzenie do administracji systemu Windows Server

- Wprowadzenie do systemu Windows Server
- Wprowadzenie do systemu Windows Server Core
- Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server
- **Ćwiczenie:** Wdrażanie i konfiguracja systemu Windows Server
 - Wdrażanie i konfiguracja systemu Server Core
 - Wdrażanie i stosowanie zdalnej administracji serwerami

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać system Windows Server, a także techniki wdrażania, serwisowania i aktywacji,
- Opisać system Windows Server Core, przedstawić jego specyfikę i sposoby administrowania nim.

Moduł 2: Usługi zarządzania tożsamością w systemie Windows Server

- Wprowadzenie do AD DS
- Wdrażanie kontrolerów domeny Windows Server
- Wprowadzenie do usługi Azure AD
- Wdrażanie zasad grupy
- Wprowadzenie do usług certyfikatów Active Directory
- **Ćwiczenie:** Wdrażanie usług zarządzania tożsamością i zasad grupy
 - Wdrażanie nowego kontrolera domeny w systemie Server Core
 - Konfigurowanie zasad grupy
 - Wdrażanie i korzystanie z usług certyfikatów
 - Wyjaśnienie podstaw zasad grupy i konfiguracja GPO w środowisku domenowym
 - Opis roli usług certyfikatów Active Directory i korzystanie z certyfikatów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać AD DS w środowisku systemu Windows Server,
- Wdrażać kontrolery domeny w AD DS,
- Opisać Azure AD i korzyści płynące z integracji Azure AD z AD DS.

Moduł 3: Usługi infrastruktury sieciowej w systemie Windows Server

- Wdrażanie i zarządzanie protokołem DHCP

- Wdrażanie i zarządzanie systemem DNS
- Wdrażanie i zarządzanie systemem IPAM
- Usługi dostępu zdalnego w systemie Windows Server
- **Ćwiczenie:** Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server
 - Wdrażanie i konfiguracja protokołu DHCP
 - Wdrażanie i konfiguracja systemu DNS
 - Wdrażanie serwera proxy aplikacji sieci WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać, wdrożyć i skonfigurować usługę DHCP,
- Wdrażać, konfigurować i zarządzać systemem DNS,
- Opisać, wdrożyć i zarządzać systemem IPAM.

Moduł 4: Serwery plików i zarządzanie pamięcią masową w systemie Windows Server

- Woluminy i systemy plików w systemie Windows Server
- Wdrażanie udostępniania w systemie Windows Server
- Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
- Wdrażanie deduplikacji danych
- Wdrażanie interfejsu iSCSI
- Wdrażanie rozproszonego systemu plików
- **Ćwiczenie:** Wdrażanie rozwiązań pamięci masowej w systemie Windows Server
 - Wdrażanie deduplikacji danych
 - Konfiguracja magazynu iSCSI
 - Konfiguracja nadmiarowych przestrzeni dyskowych
 - Wdrażanie Storage Spaces Direct

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Wdrażać udostępnianie w systemie Windows Server,
- Wdrożyć technologię Storage Spaces,
- Wdrażać funkcję deduplikacji danych,
- Wdrażać pamięć masową opartą na iSCSI,
- Wdrożyć i zarządzać rozproszonym systemem plików (DFS - Distributed File System).

Moduł 5: Virtualizacja Hyper-V i kontenery w systemie Windows Server

- Hyper-V w systemie Windows Server
- Konfiguracja maszyn wirtualnych /li>
- Zabezpieczanie virtualizacji w systemie Windows Server
- Kontenery w systemie Windows Server
- Wprowadzenie do platformy Kubernetes
- **Ćwiczenie:** Wdrażanie i konfiguracja virtualizacji w systemie Windows Server
 - Tworzenie i konfigurowanie maszyn wirtualnych
 - Instalacja i konfiguracja kontenerów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać kluczowe cechy Hyper-V w systemie Windows Server,
- Opisać ustawienia maszyn wirtualnych oraz wdrożyć i skonfigurować maszyny wirtualne w Hyper-V,
- Wyjaśnić zastosowanie technologii bezpieczeństwa w virtualizacji,

- Opisać i wdrożyć kontenery w systemie Windows Server,
- Wyjaśnić zastosowanie platformy Kubernetes w systemie Windows.

Moduł 6: Wysoka dostępność w systemie Windows Server

- Planowanie wdrożenia klastra pracy awaryjnej
- Tworzenie i konfiguracja klastra pracy awaryjnej
- Wprowadzenie do rozciągniętych klastrów
- Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V
- **Ćwiczenie:** Wdrażanie klastra pracy awaryjnej
 - Konfiguracja pamięci masowej i tworzenie klastra
 - Wdrażanie i konfiguracja serwera plików o wysokiej dostępności
 - Sprawdzanie poprawności wdrożenia serwera plików o wysokiej dostępności

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać klastry pracy awaryjnej i warunki jego wdrożenia,
- Tworzyć i konfigurować klastry pracy awaryjnej,
- Opisać klastry rozciągnięte,
- Opisać opcje osiągnięcia wysokiej dostępności za pomocą maszyn wirtualnych Hyper-V.

Moduł 7: Odzyskiwanie danych po awarii w systemie Windows Server

- Funkcja Hyper-V Replica
- Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server
- **Ćwiczenie:** Wdrażanie funkcji Hyper-V Replica i Windows Server Backup
 - Wdrażanie funkcji Hyper-V Replica
 - Wdrażanie tworzenia kopii zapasowych i przywracania za pomocą narzędzia Windows Server Backup

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać i wdrożyć funkcję Hyper-V Replica,
- Opisać usługę Azure Site Recovery,
- Opisać i wdrożyć narzędzie Windows Server Backup,
- Opisać usługę Azure Backup.

Moduł 8: Bezpieczeństwo systemu Windows Server

- Ochrona danych uwierzytelniających i dostępu uprzywilejowanego
- Hardening systemu Windows Server
- JEA w systemie Windows Server
- Zabezpieczanie i analiza ruchu w SMB
- Zarządzanie aktualizacjami w systemie Windows Server
- **Ćwiczenie:** Konfiguracja zabezpieczeń w systemie Windows Server
 - Konfiguracja funkcji Windows Defender Credential Guard
 - Lokalizowanie problematycznych kont
 - Wdrażanie rozwiązania LAPS

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać dane uwierzytelniające wykorzystywane w systemie Windows Server,
- Wyjaśnić, jak wdrożyć zabezpieczenia dostępu uprzywilejowanego,
- Opisać metody i technologie hardeningu zabezpieczeń w systemie Windows Server,
- Opisać i skonfigurować usługę Just Enough Administration (JEA),
- Zabezpieczyć ruch SMB w systemie Windows Server,

- Opisać usługę Windows Update oraz jej opcje wdrażania i zarządzania.

Moduł 9: RDS (usługi pulpitu zdalnego) w systemie Windows Server

- Wprowadzenie do RDS
- Konfiguracja wdrażania pulpitu opartego na sesji
- Wprowadzenie do osobistych i połączonych pulpituów wirtualnych
- **Ćwiczenie:** Wdrażanie RDS w systemie Windows Server
 - Wdrażanie RDS
 - Konfigurowanie ustawień kolekcji sesji i wykorzystywanie RDC
 - Konfiguracja szablonu pulpitu wirtualnego

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać usługi Remote Desktop Services (RDS - usługi pulpitu zdalnego) w systemie Windows Server,
- Opisać i wdrożyć pulpity oparte na sesji,
- Opisać osobiste i połączone pulpity wirtualne.

Moduł 10: Dostęp zdalny i usługi internetowe w systemie Windows Server

- Wdrażanie sieci VPN
- Wdrażanie usługi Always On VPN
- Wdrażanie systemu NPS
- Wdrażanie serwera WWW w systemie Windows Server
- **Ćwiczenie:** Wdrażanie obciążeń sieciowych
 - Wdrażanie sieci VPN w systemie Windows Server
 - Wdrażanie i konfiguracja serwera WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać opcje sieci VPN w systemie Windows Server,
- Opisać funkcję Always On VPN,
- Opisać i skonfigurować NPS,
- Opisać i skonfigurować serwer WWW (IIS).

Moduł 11: Monitorowanie serwera i wydajności w systemie Windows Server

- Wprowadzenie do narzędzi do monitorowania systemu Windows Server
- Korzystanie z monitora wydajności
- Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów
- **Ćwiczenie:** Monitorowanie i rozwiązywanie problemów z systemem Windows Server
 - Ustanowienie bazowego poziomu wydajności
 - Identyfikacja źródła problemu z wydajnością

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia monitorujące w systemie Windows Server,
- Opisać monitorowanie wydajności i wykorzystać je w systemie Windows Server,
- Opisać rejestrowanie zdarzeń i monitorować rejestrowanie zdarzeń dla celów rozwiązywania problemów.

Moduł 12: Aktualizacja i migracja w systemie Windows Server

- Migracja AD DS
- Usługa migracji pamięci masowej
- Narzędzia do migracji systemu Windows Server
- **Ćwiczenie:** Migracja obciążeń serwera
 - Wdrażanie usługi migracji pamięci masowej

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia, których należy użyć do migracji AD DS,
- Opisać usługę migracji pamięci masowej,
- Opisać narzędzia do migracji Windows Server i scenariusze ich użycia.

Część 4:

Szkolenie przeznaczone dla administratora Active Directory w Microsoft Windows Server 2019/2022

Przedmiotem zamówienia jest realizacja szkolenia technicznego trwającego minimum dwa dni (2 x 8h) skierowanego do administratora systemów serwerowych odpowiedzialnego za utrzymanie i zarządzanie usługą katalogową w środowisku serwerowym. Szkolenie powinno obejmować tematykę instalacji i konfiguracji kontrolerów domeny, zarządzania kontami użytkowników i zasobami katalogowymi, wdrażania struktur organizacyjnych, konfiguracji replikacji, a także stosowania zasad grupy (Group Policy) do automatyzacji i standaryzacji środowiska użytkowników m.in.:

Moduł 1: Instalacja i konfiguracja kontrolerów domeny

- Omówienie usług AD DS
- Omówienie kontrolerów domeny usług AD DS
- Wdrożenie kontrolera domeny
- Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022

Moduł 2: Zarządzanie obiektami w AD DS

- Zarządzanie kontami użytkowników
- Zarządzanie grupami w usługach AD DS
- Zarządzanie obiektami typu komputer w AD DS
- Wdrażanie i zarządzanie OU

Moduł 3: Zarządzanie zaawansowaną infrastrukturą AD DS

- Wprowadzenie do zaawansowanych wdrożeń AD DS
- Wdrożenie rozproszonego środowiska AD DS
- Konfiguracja relacji zaufania AD DS

Moduł 4: Wdrażanie i zarządzanie lokacjami i repliką AD DS

- Omówienie replikacji usług AD DS
- Konfigurowanie lokacji usług AD DS
- Konfigurowanie i monitorowanie replikacji usług AD DS

Moduł 5: Wdrażanie zasad grupy

- Wprowadzenie do zasad grupy
- Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)
- Konfiguracja zakresu i przetwarzania obiektów GPO
- Rozwiązywanie problemów z GPO

Moduł 6: Zarządzanie ustawieniami użytkowników za pomocą zasad grupy

- Wdrażanie szablonów administracyjnych
- Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
- Konfiguracja preferencji zasad grupowych

W przypadku tego szkolenia Zamawiający dopuszcza możliwość przeprowadzenia go w formie zdalnej (online).

II. Termin wykonania:

Szkolenia należy przeprowadzić do dnia 30 kwietnia 2026 r.

III. Składanie ofert:

1. Ofertę prosimy złożyć/przesać:

- za pośrednictwem e-Platformy: <https://platformazakupowa.pl/transakcja/1232935>
do dnia 29.01.2026r.

2. Termin związania ofertą wynosi: 30 dni.

IV. Kryterium oceny ofert:

Cena oferty brutto – 100%

Liczba punktów w kryterium „Cena oferty brutto (C)” zostanie obliczona według wzoru:

$$C = \frac{C_{min}}{C_{bad}}$$

gdzie:

- C_{min} – najniższa cena spośród wszystkich ofert,
- C_{bad} – cena badanej oferty,
- C – liczba punktów w kryterium

V. Warunki udziału w postępowaniu:

- 1) O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).

VI. Sposób przygotowania oferty:

Ofertę należy przygotować na Formularzu ofertowym stanowiącym załącznik nr 1 do zapytania.

VII. Odrzucenie ofert / Unieważnienie postępowania:

Zamawiający dopuszcza możliwość unieważnienia postępowania bez podania przyczyny.

VIII. Negocjacje:

Zamawiający dopuszcza możliwość przeprowadzenia negocjacji złożonych ofert.

IX. Zapytania i wyjaśnienia do treści zapytania ofertowego:

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego.
2. Zamawiający może dokonać odpowiednich wyjaśnień i ewentualnych zmian lub też może pozostawić wniosek bez rozpoznania, w szczególności jeżeli treść zapytań wpłynęły na co najmniej jeden dzień przed terminem składania ofert.
3. Treść zapytań wraz z wyjaśnieniami i ewentualnymi zmianami Zamawiający przekaze Wykonawcom, którym przekazał zaproszenie do złożenia oferty.

X. Inne wymagania Zamawiającego wobec wykonawcy:

Zamawiający wymaga, aby Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza, przedstawił projekt umowy w sprawie zamówienia publicznego. Projekt umowy musi zostać sporządzony w oparciu o treść oferty Wykonawcy oraz musi uwzględniać wszystkie **Istotne Postanowienia Umowy (IPU)** określone przez Zamawiającego w załączniku nr 1 do Zaproszenia. Wykonawca zobowiązany jest dostarczyć projekt umowy do akceptacji Zamawiającego w terminie 4 dni roboczych od dnia zawiadomienia o wyborze oferty.

XI. Załączniki:

1. Istotne warunki zamówienia.
2. Formularz ofertowy.

*Burmistrz Miasta i Gminy Sztum
z up.
mgr Małgorzata Surdyka
Sekretarz Miasta i Gminy Sztum*