SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Przedmiot zamówienia:

„Dostawa urządzeń komputerowych w ramach realizacji projektu – Cyberbezpieczna Gmina Sławno”

Nazwa Zamawiającego:

Gmina Sławno
REGON: 770979909
NIP: 499-052-36-66
Adres: ul. I Pułku Ułanów 11, 76 – 100 Sławno
Strona internetowa: www.gminaslawno.pl
Strona prowadzonego postępowania:
https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-1f7835df-355f-4af2-99c9-1e152342f933
Godziny urzędowania: poniedziałki: 8.00 – 16.00, od wtorku do piątku: 7.00 – 15.00
Jednostka prowadząca postępowanie:
Urząd Gminy Sławno
ul. I Pułku Ułanów 11
76 – 100 Sławno
E-mail: sekretariat@gminaslawno.pl
Adres skrzynki ePUAP: /gminaslawno/skrytka
Nr telefonu: 0 59 810 75 26
Nr faksu: 0 59 810 75 26

ZATWIERDZAM

Krzysztof Jan Jędrzejczyk

Elektronicznie podpisany przez Krzysztof Jan Jędrzejczyk
Data: 2025.07.03 10:14:22 +02'00'

Sławno, dnia 3 lipca 2025 r.

SPIS TREŚCI

ROZDZIAŁ I. TRYB UDZIELENIA ZAMÓWIENIA PUBLICZNEGO ORAZ MIEJSCA, W KTÓRYCH ZOSTAŁO ZAMIESZCZONE OGŁOSZENIE O ZAMÓWIENIU.

1. Postępowanie o udzielanie zamówienia publicznego prowadzone jest w trybie podstawowym na podstawie art. 275 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2024, poz. 1320 z późn. zm.) zwanej dalej ustawą Pzp oraz aktów wykonawczych do tej ustawy.
2. Miejsce publikacji ogłoszenia o zamówieniu:
   a) Biuletyn Zamówień Publicznych;
   b) strona prowadzonego postępowania:
   https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-1f7835df-355f-4af2-99c9-1e152342f933
   na której udostępniane będą również zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia.

ROZDZIAŁ II. INFORMACJA DOTYCZĄCA MOŻLIWOŚCI PROWADZENIA NEGOCJACJI.

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

ROZDZIAŁ III. OPIS PRZEDMIOTU ZAMÓWIENIA.

1. Przedmiotem zamówienia jest dostawa urządzeń komputerowych w ramach realizacji projektu „Cyberbezpieczna Gmina Sławno”.
2. Przedmiot zamówienia podzielony został na dwie części:
   1) **Część nr 1 –** „Dostawa serwerów, macierzy pamięci masowej, systemów operacyjnych wraz z usługami oraz zasilaczy awaryjnych”;
   2) **Część nr 2 –** „Rozszerzenie obecnego UTM o funkcję HA wraz z wdrożeniem, dostawa systemu bezpiecznego zdalnego dostępu wraz z wdrożeniem, systemu do kontroli poczty elektronicznej wraz z wdrożeniem. Dostawa przełączników sieciowych. Dostawa, wdrożenie i konfiguracja NAC”.
3. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.
4. **Wymagania ogólne:**
   1) O ile inaczej nie zaznaczono, wszelkie zapisy SWZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
   2) Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2024 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie „fabrycznie nowy” należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez „wadę fizyczną” należy rozumieć również jakąkolwiek niezgodność ze opisem przedmiotu zamówienia.
   3) Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania software’owe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu.

4) Dokumenty gwarancyjne wystawiane i przekazywane przez Wykonawcę powinny być zgodne z zapisami SWZ.
5) Oprogramowanie pochodzić będzie z legalnego, tj. akceptowanego przez producenta Oprogramowania kanału dystrybucji oraz zostanie udostępnione Zamawiającemu do korzystania na warunkach stosowanych lub akceptowanych przez takiego producenta.

5. **Kryteria równoważności:**
   1) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
   2) W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm polskich lub europejskich, ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 5 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
   3) Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SWZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

6. **<u>Część nr 1 – Dostawa serwerów, macierzy pamięci masowej, systemów operacyjnych wraz z usługami oraz zasilaczy awaryjnych:</u>**
   1) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
   2) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
   3) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
   4) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
   5) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
   6) Urządzenia na etapie dostawy pomiędzy producentem, a zamawiającym nie mogą podlegać modyfikacjom.
   7) Cały zaoferowany sprzęt (dwa serwery i macierz) musi posiadać jeden punkt świadczenia napraw gwarancyjnych.
   8) **<u>Serwer – 2 szt. – wymagania minimalne:</u>**
      a) **Obudowa –** obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5”; wyposażona w panel LCD umieszczony na froncie obudowy,

umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze; obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.

b) **Płyta główna –** płyta główna z możliwością zainstalowania do dwóch procesorów; obsługa procesorów 32 rdzeniowych; musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym; na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci; powinna obsługiwać do 1TB pamięci RAM.
c) **Chipset –** dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
d) **Procesor –** zainstalowane dwa procesory 12-rdzeniowe, min. 2.4 GHz (częstotliwość bazowa), klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 239 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
e) **RAM –** min. 256 GB DDR5 RDIMM 5600MT/s w kościach 64GB.
f) **Gniazda PCI –** min. dwa sloty PCIe generacji 5.
g) **Kontroler RAID –** sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10.
h) **Dyski twarde –** zainstalowane 2 x dysk SSD SATA o pojemności min. 480 GB, 6Gb, 2,5“ Hot-Plug; możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.
i) **Interfejsy sieciowe/FC/SAS –** wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT; 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe); 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28; w zestawie z serwerem muszą znajdować się 2 kable DAC 10GbE SFP+/SFP+ min. 3 m, dostarczone przez producenta serwera; w zestawie z serwerem wykonawca dostarczy 3 patchcordy RJ-45 cat 6 o długości minimum 3 m.
j) **Elementy montażowe –** komplet wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych; ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych.
k) **Wbudowane porty –** 4 porty USB w tym min:
   – 1 port USB 3.0 z tyłu obudowy,
   – 1 port micro USB z przodu obudowy,
   – 2 x port VGA z czego jeden z przodu obudowy,
   – możliwość rozbudowy o port RS232m.
l) **Video –** zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
m) **Zasilacze –** Redundantne, Hot-Plug min. 1100 W klasy Titanium.
n) **System operacyjny/dodatkowe oprogramowanie –** fabrycznie zainstalowany system operacyjny Microsoft Windows Serwer 2025 Standard:
   – licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze,
   – dostarczona z serwerem licencja musi uprawniać do uruchomienia w środowisku wirtualnym co najmniej sześciu systemów Windows Server 2025,

- licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo,
- dodatkowe licencje – serwery muszą zostać dostarczone z licencjami CAL dostarczonymi przez producenta oferowanych serwerów – łącznie 50 licencji na użytkownika Windows Server 2025 (Windows Server 2025 User CAL).

o) **Bezpieczeństwo –** zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych; możliwość wyłączenia w BIOS funkcji przycisku zasilania; BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła; wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą; moduł TPM 2.0; możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera; możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem; serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania; ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155; jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust); wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji; mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.

p) **Karta Zarządzania –** niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
- możliwość podmontowania zdalnych wirtualnych napędów;
- wirtualną konsolę z dostępem do myszy, klawiatury;
- wsparcie dla IPv6;
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- integracja z Active Directory;
- możliwość obsługi przez dwóch administratorów jednocześnie;
- wsparcie dla automatycznej rejestracji DNS;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;

- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera;
- z możliwością rozszerzenia funkcjonalności o: wirtualny schowek ułatwiający korzystanie z konsoli zdalnej; przesyłanie danych telemetrycznych w czasie rzeczywistym; dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze; automatyczna rejestracja certyfikatów (ACE).

q) **Oprogramowanie do zarządzania –** możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:
- wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
- integracja z Active Directory;
- możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
- wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish;
- możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
- szczegółowy opis wykrytych systemów oraz ich komponentów;
- możliwość eksportu raportu do CSV, HTML, XLS, PDF;
- możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu;
- grupowanie urządzeń w oparciu o kryteria użytkownika;
- tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji;
- możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach;
- szybki podgląd stanu środowiska;
- podsumowanie stanu dla każdego urządzenia;
- szczegółowy status urządzenia/elementu/komponentu;
- generowanie alertów przy zmianie stanu urządzenia;
- filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
- integracja z service desk producenta dostarczonej platformy sprzętowej;
- możliwość przejęcia zdalnego pulpitu;
- możliwość podmontowania wirtualnego napędu;
- kreator umożliwiający dostosowanie akcji dla wybranych alertów;
- możliwość importu plików MIB;
- przesyłanie alertów „as-is” do innych konsol firm trzecich;
- możliwość definiowania ról administratorów;
- możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów;
- aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
- możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta;

- możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
- moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera;
- możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności;
- wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile;
- możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami;
- tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta;
- zdalne uruchamianie diagnostyki serwera;
- dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym;
- oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

r) **Certyfikaty** – serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001; serwer musi posiadać deklaracja CE; oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć; wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne; usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC; produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu; we wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC; potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – Wykonawca złoży dokument potwierdzający spełnianie wymogu; oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.

s) **Dokumentacja użytkownika –** Zamawiający wymaga dokumentacji w języku polskim lub angielskim; możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

t) **Warunki gwarancji –** Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat; Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet; Zamawiający wymaga pojedynczego punktu

kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania; Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy; Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki; naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę; Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego; Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego; możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii; charakterystyka usługi diagnostyki:

- możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego;
- po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu; jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy;
- reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową;
- pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu;
- jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej; technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

9) **<u>Dodatkowa karta dla posiadanego serwera – 1 szt. – wymagania minimalne –</u>** należy dostarczyć nową kartę sieciową dwuportową 25Gb SFP28 niskoprofilową,

zatwierdzoną do pracy w serwerze Dell R550 przez producenta tego serwera; karta musi pochodzić z autoryzowanej dystrybucji producenta serwera.

10) **Macierz – 1 szt. – wymagania minimalne:**
   a) **Typ obudowy –** macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5”.
   b) **Przestrzeń dyskowa –** zainstalowane 11 x dysk SSD SAS o pojemności min. 1.92 TB, Hot-Plug, 1 DWPD.
   c) **Możliwość rozbudowy –** macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
   d) **Obsługa dysków** – macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS; macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej.
   e) **Sposób zabezpieczenia danych –** macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping); macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID; macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku); macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
   f) **Tryb pracy kontrolerów macierzowych –** macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe; wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
   g) **Pamięć cache –** macierz musi posiadać minimum sumarycznie 32 GB pamięci cache; pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM; pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi; dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
   h) **Rozbudowa pamięci cache –** macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash; jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
   i) **Interfejsy –** macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI w standardzie SFP28 (4 porty na kontroler); w zestawie musi znajdować się 6 kabli DAC 25GbE SFP28/SFP28 min. 3 m, dostarczonych przez producenta macierzy.
   j) **Zarządzanie –** zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego; zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.

k) **Zarządzanie grupami dyskowymi oraz dyskami logicznymi –** macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej; musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide – striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy; jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

l) **Thin Provisioning –** macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning; macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin; proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP); jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

m) **Tiering –** macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS; Tiering musi obejmować wszystkie woluminy w danej puli dyskowej; dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.

n) **Wewnętrzne kopie migawkowe –** macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych; kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii; zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii; macierz musi wspierać minimum 512 kopii migawkowych; jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

o) **Wewnętrzne kopie pełne –** macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych; jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

p) **Migracja danych w obrębie macierzy –** macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów; zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy; jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.

q) **Zdalna replikacja danych –** macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny; replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy; jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.

r) **Podłączanie zewnętrznych systemów operacyjnych –** macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami); macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix; dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów; dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych; jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.

s) **Redundancja –** macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych; musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów; macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory; macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy; zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.

t) **Dodatkowe wymagania –** oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej; niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych; za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych; możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.

u) **Standardy bezpieczeństwa –** urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International).

v) **Inne –** urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta; na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta; wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001; Deklaracja zgodności CE.

w) **Warunki gwarancji –** Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat; Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet; Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania; Zamawiający oczekuje możliwości samodzielnego

kwalifikowania poziomu ważności naprawy; Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki; naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę; Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego; Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego; wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

11) **<u>Wdrożenie oprogramowania, uruchomienie, instalacja i konfiguracja serwerów, macierzy dyskowej – 1 kpl. – wymagania minimalne:</u>**
   a) Usługa wdrożenia musi obejmować montaż dostarczonej karty sieciowej w posiadanym przez zamawiającego serwerze Dell R550.
   b) Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego, a także odpowiednie redundantne połączenie oferowanych serwerów z macierzą.
   c) Na oferowanych urządzeniach musi zostać przeprowadzona aktualizacja firmware’u. Urządzenia zostaną skonfigurowane zgodnie z najlepszymi praktykami (w tym zasób dyskowy na macierzy dla podłączonych serwerów), a na oferowanych serwerach zainstalowane zostanie oprogramowanie do wirtualizacji (Windows Server Hyper-V) wraz z obsługą klastra trybu failover.
   d) Przy wykorzystaniu zaoferowanych licencji Microsoft muszą zostać utworzone nowe maszyny wirtualne z systemem Windows Server 2025 Standard. Maszyny należy uruchomić w ramach klastra trybu failover.
   e) Wszystkie wymienione prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym.
   f) Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.
   g) Wykonawca powinien posiadać certyfikaty z firm, których rozwiązania wdraża.
12) **<u>Zasilacz awaryjny serwerowy – 2 szt. – wymagania minimalne:</u>**
   a) **Wymagania techniczne dla jednostki UPS –** moc znamionowa jednostki nie mniej niż 3000VA / 2700W; wersja do montażu w szafie Rack – szyny montażowe w zestawie; technologia podwójnej konwersji (online); temperatura eksploatacji 0 - 40 °C; wilgotność względna podczas pracy 0 - 95 %; wysokość n.p.m. podczas pracy 0-3000 m; rozpraszanie ciepła w trybie online ≤703,00 BTU/h; sprawność: klasa ochrony IP 20, klasa energetyczna sprzętu przeciwprzepięciowego 340J.

b) **Parametry wejściowe –** nominalne napięcie wejściowe 230V; częstotliwość wejściowa 40–70 Hz; typ gniazda wejściowego: IEC-320 C20; zmienny zakres napięcia wejściowego w trybie podstawowym (pełne obciążenie) 160 – 275 V; (połowa obciążenia) 100 – 275V.

c) **Parametry wyjściowe –** napięcie wyjściowe 230V; częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz ±3Hz; inne napięcia wyjściowe 220, 240 V (nastawa z wyświetlacza); współczynnik szczytu 3:1; typ przebiegu sinusoida; złącza/gniazda wyjściowe; 8 szt. IEC 320 C13; 2 szt. IEC 320 C19; układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny).

d) **Akumulatory i czas podtrzymania –** typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny; czas autonomii: 3 minuty 58 sekund dla pełnego obciążenia, 11 minut 48 sekund dla połowy obciążenia; typowy czas ładowania 3 godziny; oczekiwana żywotność akumulatora (lata) 3 – 5; baterie wymieniane na gorąco; możliwość rozszerzenia czasu podtrzymania poprzez dodanie do 10 zewnętrznych modułów akumulatorowych.

e) **Komunikacja i zarządzanie –** gniazdo do montażu karty WEB/SNMP – Smart Slot x1 (Zasilacz dostarczany wraz z kartą zarządzania sieciowego); porty komunikacyjne – serial (RJ-45), Smart-Slot, USB (typ A); panel sterowania – wielofunkcyjna konsola sterownicza i informacyjna LCD; alarm dźwiękowy – alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia; awaryjny wyłącznik zasilania (EPO).

f) **Certyfikaty, zgodności oraz gwarancja –** CE, EN/IEC 62040-1, EN/IEC 62040-2, VDE, RoHS, REACh; 3 lata gwarancji producenta door to door.

g) **Oprogramowanie –** dostępne oprogramowanie do zarządzania/monitoringu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.

13) **<u>Zasilacz awaryjny – 13 szt. – wymagania minimalne:</u>**

a) **Minimalne wymagania techniczne dla jednostki UPS –** moc znamionowa jednostki nie mniej niż 540W / 900VA; topologia line-interactive; temperatura eksploatacji 0 - 40 °C; wilgotność względna podczas pracy 0 - 95 %; klasa energetyczna sprzętu przeciwprzepięciowego 613 J; automatyczna regulacja napięcia (AVR).

b) **Parametry wejściowe –** nominalne napięcie wejściowe 230V; zakres napięcia wejściowego 176 – 294 V; częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie); standard wtyczki: CEE 7/7P.

c) **Parametry wyjściowe –** napięcie wyjściowe 230V; częstotliwość na wyjściu 50/60Hz +/- 1 Hz; typ przebiegu – schodkowa aproksymacja sinusoidy; RJ11 zabezpieczenie przeciwprzepięciowe sieci fax/tel; złącza/gniazda wyjściowe – 3 gniazda Francuskie z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania, 3 gniazda Francuskie z zabezpieczeniem przeciwprzepięciowym.

d) **Akumulatory i czas podtrzymania –** typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu; czas autonomii – 4 minuty 38 sekund dla pełnego obciążenia, 16 minut 18 sekund dla połowy

obciążenia; typowy czas ładowania 8 godzin; oczekiwana żywotność akumulatora (lata) 3 – 5; baterie wymieniane na gorąco.

e) **Komunikacja i zarządzanie –** gniazda RJ45 (Gigabit), USB&Serial; ekran LCD informujący o statusie pracy oraz poziomie naładowania akumulatorów; alarm dźwiękowy – praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, wykrycie wymiany akumulatora.

f) **Certyfikaty, zgodności oraz gwarancja –** CE, RoHS, REACh; 3 lata gwarancji producenta door to door.

g) **Oprogramowanie –** oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące:
   - monitorowania i zarządzania zasilaczy UPS,
   - bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem,
   - bezpieczny dostęp do internetowego interfejsu użytkownika (UI),
   - możliwość dokładnego określania czasu i sekwencji wyłączania za pomocą dziennika zdarzeń,
   - identyfikacja potencjalnych zagrożeń, możliwość eksportowania dziennika zdarzeń.

7. **Część nr 2 – Rozszerzenie obecnego UTM o funkcję HA wraz z wdrożeniem, dostawa systemu bezpiecznego zdalnego dostępu wraz z wdrożeniem, systemu do kontroli poczty elektronicznej wraz z wdrożeniem. Dostawa przełączników sieciowych. Dostawa, wdrożenie i konfiguracja NAC:**

   1) **Urządzenie HA do obecnego urządzenia UTM z systemem montażu umożliwiającym mocowanie w szafie serwerowej – wymagania minimalne –** dostawa dodatkowego urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym Sonicwall TZ570; urządzenie standby powinno mieć identyczne parametry wydajnościowe oraz sprzętowe jak podstawowa jednostka; urządzenia powinny synchronizować pomiędzy sobą stany sesji połączeń; obecne urządzenie to Sonicwall TZ570; uruchomienie systemu HA; weryfikacja reguł na obecnym urządzeniu UTM.

   2) **System bezpiecznego zdalnego dostępu – wymagania minimalne:**
      - Licencja wieczysta na oprogramowanie do bezpiecznego zdalnego dostępu z interfejsem graficznym jednolitym z urządzeniem UTM.
      - Zapewniające równoczesny zdalny dostęp 15 osobom.
      - Oprogramowanie musi posiadać wsparcie producenta do 30.06.2026 r.
      - Wdrożenie.

   3) **System do kontroli poczty elektronicznej – wymagania minimalne:**
      a) **Wymagania ogólne:**
         - System ochrony poczty musi działać w środowisku hostowanym poza infrastrukturą klienta na terenie Unii Europejskiej.
         - System powinien funkcjonować jako Proxy ze wsparciem dla protokołu SMTP.
         - System powinien posiadać własne filtry reputacji oraz mechanizmy antyphishingowe oraz antyspamowe.
         - System powinien umożliwiać skanowanie przychodzącej i wychodzącej.

- Możliwość wykorzystania rekordów SPF oraz mechanizmu DKIM oraz DMARC.
- Automatyczna aktualizacja filtrów bez przerywania pracy.
- Musi posiadać wewnętrzną konsolę do administrowania (Web), bez potrzeby instalowania klientów.
- Możliwość stworzenia kwarantanny per użytkownik. Umożliwianie użytkownikowi zarządzania własną kwarantanną, usuwanie wiadomości lub zwolnienie tych, które nie uważają za SPAM, a także możliwość blokowania e-maili. Kwarantanna może być implementowana z bezpośrednią integracją z aplikacji poczty e-mail lub przez interfejs WWW (HTTPS).
- Możliwość uruchomienia konsoli web, dzięki której użytkownicy mogą sprawdzać wiadomości, które są poddawane kwarantannie ze względu na spam.
- Możliwość, aby użytkownicy sami tworzyli listy wyjątków dla nadawców w konsoli web.
- Umożliwianie użytkownikom na przeglądanie podejrzanych wiadomości w kwarantannie i zaakceptowanie nadawców bez interwencji administratora.
- Umożliwianie użytkownikowi na utworzenie osobistych, białych list (zaufanych adresów), niezależnie od administratora, tak aby te białe listy nie kolidowały z filtrami innych użytkowników.
- Moduł kwarantannowy powinien znajdować się w samym systemie antyspamowym i być w stanie wysłać okresowe powiadomienie do użytkowników, informując o wiadomościach traktowanych jako SPAM, które zostały wstawione do kwarantanny.
- Użytkownik powinien być w stanie automatycznie usunąć wiadomości poddane kwarantannie zgodnie z ustawieniami określonymi przez administratora.
- System powinien dawać możliwość powiadomienia administratora pocztą e-mail, jeśli filtry antyspamowe nie otrzymują aktualizacji przez pewien czas. Przyjmuje się alternatywnie, że administrator zostanie powiadomiony w przypadku błędów aktualizacji.
- Rozwiązanie powinno być w stanie tworzyć i zarządzać wieloma grupami użytkowników i definiować zróżnicowane reguły i polityki dla każdej z tych grup. System powinien integrować się z bazą LDAP.
- Rozwiązanie umożliwia stosowanie filtrów, które aplikowane są przed wejściem wiadomości do systemu. Filtry te muszą mieć możliwość klasyfikacji różnych typów zachowań (takich jak białe i czarne listy). Filtry połączeń muszą być konfigurowane przynajmniej przez: adres IP; zakres adresów IP; muszą wspierać RBL (listy oparte o DNS); muszą posiadać i mieć możliwość używania filtrów reputacji; muszą być w stanie definiować następujące polityki: limit ilości odbiorców na wiadomość, limit wielkości wiadomości; pozwalać lub zabraniać używania SSL/ TSL dla połączeń; używać antyspam; musi wpierać SSL / TLS dla połączeń przychodzących i wychodzących; musi mieć możliwość używania odwrotną translację adresów DNS (revDNS); urządzanie powinno wspierać wiele domen (rekordów MX).

- Kolejki dostarczania w oprogramowaniu MTA muszą być na tyle duże, aby wspierać przeładowanie wiadomościami w sytuacji awarii albo problemów w innych punktach infrastruktury pocztowej.
- Rozwiązanie powinno wspierać unikalne profile, które obsługują zachowanie wiadomości odbijanych bazując na domenach lub na docelowych adresach IP.
- Moduł kwarantanny powinien być w stanie wysłać okresowe powiadomienie dla użytkowników, informując o wiadomościach traktowanych jako spam, które zostały przeniesione do kwarantanny.
- Directory Collection Protection: rozwiązanie musi posiadać ochronę przed tego typu atakami dzięki skanowaniu odbiorcy wiadomości w LDAP, Active Directory.
- DoS: system operacyjny urządzenia fizycznego lub wirtualnego powinien mieć możliwość identyfikacji i ochrony MTA przed atakami typu DoS.
- System uwierzytelniania powinien mieć ochronę przed atakami (np. atak słownikowy).
- Posiadać funkcję zapory e-mail, chroniąc serwer poczty przed atakiem typu Directory Harvest Attack (DHA).
- Filtry ochrony przed spamem powinny skanować wszystkie części wiadomości, w tym: nadawcy (komenda SMTP MAIL FROM), odbiorcy (komenda SMTP RCPT TO), nagłówek wiadomości, treść wiadomości e-mail, załączniki widomości e-mail.
- Filtry bezpieczeństwa: urządzenie musi posiadać mechanizm identyfikacji treści wiadomości takich elementów jak: numer karty kredytowej, RG i / lub CPF; musi posiadać mechanizmy tworzenia katalogów słów należących do konkretnych tematów, takich jak przestępstwa; musi zezwalać na heurystyczną weryfikację nowo wprowadzonych wirusów, nawet bez dostępnej szczepionki; musi pozwalać na weryfikację rzeczywistego typu pliku nawet po zmianie nazwy; umożliwiać skanowanie plików wykonywalnych skompresowanych; posiadać ochronę przed oprogramowaniem szpiegującym bez potrzeby dodatkowego oprogramowania lub agenta; ochrona przed Dialerami bez potrzeby dodatkowego oprogramowania lub agenta.
- Rozwiązanie powinno umożliwiać wysyłanie plików do dodatkowej analizy w systemie sandbox przy czym system sandbox powinien posiadać co najmniej cztery równolegle działające silniki w tym dwa pochodzące od innego producenta.
- System powinien umożliwiać weryfikację linków zawartych w wiadomościach nawet po dostarczeniu wiadomości do adresata.
- System powinien umożliwiać zablokowanie załączniku których zaszyfrowanych hasłem.
- System powinien umożliwiać wykonanie akcji na wiadomościach takich jak: przesłanie do JunkBox; otagowanie tematu; dodatnie zdefiniowanego przez administratora nagłówka; usunięcie dowolnego nagłówka; dodanie tekstu do wiadomości; odrzucenie wiadomości; przekierowanie wiadomości do innego serwera IP; pominięcie skanowania Sanbox-a.

b) **Licencje**:

- System powinien zostać dostarczony w licencjami do ochrony 50 skrzynek pocztowych.
- Licencje powinny zapewniać ochronę antyspam, antyphising, antywirus, sandboxing oraz wsparcie techniczne 24x7 ora na okres do 30.06.2026 r.
- System powinien posiadać jednolity interfejs z obecnym rozwiązaniem do ochrony styku lokalnej sieci z Internetem.

c) **Wdrożenie.**

4) **<u>Przełącznik 48 portów wraz z rocznym wsparciem, kablem zasilającym i 4 kompatybilnymi wkładkami SFP 10 GB – 2 szt. – wymagania minimalne</u>**:

a) **Wymagania podstawowe:**

- Przełącznik wyposażony w 48 portów 10/100/1000BASE-T.
- Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex.
- Przełącznik musi być wyposażony w 8 portów uplink SFP+ 1/10G. Jeśli do pracy w trybie 10G wymagana jest licencja, to musi być ona dostarczona.
- Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet.
- Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów.
- Wszystkie porty przełącznika muszą mieć możliwość wsparcia szyfracji MACsec 128/256-bit. Jeśli funkcjonalność wymaga dodatkowej licencji, to nie musi być ona dostarczona.
- Wysokość urządzenia 1U montowana w standardowym 19” Rack.
- Przełącznik musi posiadać wbudowany zasilacz 230V.
- Przełącznik musi posiadać możliwość łączenia z innymi przełącznikami w stos z wydajnością min. 40 Gb/s.
- Przełącznik musi umożliwiać stworzenie stosu złożonego z 8 przełączników.
- Stos musi zachowywać się jak jedno urządzenie logiczne, a w szczególności mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem.
- Porty przełącznika, używane do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty transmisji danych SFP+ z przepustowością 10 Gb/s.
- Nieblokująca architektura o wydajności przełączania min. 256 Gb/s.
- Szybkość przełączania min. 190 Milionów pakietów na sekundę.
- Temperatura pracy przełącznika w zakresie min. 0^{o} do 50^{o} C.
- Tablica MAC adresów min. 32 tys.
- Pamięć operacyjna: min. 1 GB pamięci DRAM.
- Pamięć flash: min. 1 GB pamięci Flash.
- Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
- Obsługa funkcjonalności Private VLAN – blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
- Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
- Obsługa Q-in-Q IEEE 802.1ad.
- Obsługa Quality of Service: rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p; rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ; 8 kolejek priorytetów na każdym porcie

wyjściowym; obsługa kolejek Strict Priority; obsługa kolejek Weighted Round Robin; obsługa WRED (Weighted Random Early Detection).
- Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
- Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
- Obsługa CDPv2.
- Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
- Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
- Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash.
- Możliwość monitorowania zajętości CPU oraz pamięci.
- Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
- Obsługa Wirtualnych Routerów – możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
- Dedykowany port konsoli szeregowej RJ45.
- Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika.

b) **Obsługa Routingu IPv4 –** sprzętowa obsługa routingu IPv4 – forwarding; pojemność sprzętowej tabeli routingu min. 8 000 wpisów; routing statyczny; obsługa routingu dynamicznego IPv4: RIP v1/v2, OSPFv2 – możliwość rozszerzenia przez licencje, BGPv4 – możliwość rozszerzenia przez licencje, IS-IS – możliwość rozszerzenia przez licencje; Policy Based Routing dla IPv4; obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów.

c) **Obsługa Routingu IPv6 –** sprzętowa obsługa routingu IPv6 – forwarding; pojemność tabeli routingu min. 4 000 wpisów; routing statyczny; obsługa routingu dynamicznego dla IPv6: RIPng, OSPF v3 – możliwość rozszerzenia przez licencje, BGPv4 – możliwość rozszerzenia przez licencje, IS-IS – możliwość rozszerzenia przez licencje; obsługa 6to4 (RFC 3056); obsługa MLDv1 (Multicast Listener Discovery version 1); obsługa MLDv2 (Multicast Listener Discovery version 2); Policy Based Routing dla IPv6; opcja IPv6 Router Advertisement dla DNS – RFC 6106.

d) **Obsługa Multicastów –** statyczne przyłączanie do grupy multicast; filtrowanie IGMP; obsługa PIM-SM; obsługa PIM-DM – możliwość rozszerzenia przez licencje; obsługa PIM-SSM – możliwość rozszerzenia przez licencje; obsługa Multicast VLAN Registration – MVR; obsługa IGMP v1 – RFC 1112; obsługa IGMP v2 – RFC 2236; obsługa IGMP v3 – RFC 3376; obsługa IGMP v1/v2/v3 snooping; możliwość konfiguracji statycznych tras dla Routingu Multicastów.

e) **Bezpieczeństwo –** obsługa logowania do sieci Network Login: IEEE 802.1x based Network Login, MAC based Network Login, Web-based Network Login; obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants); obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation; przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication – RFC 3580; automatyczne wytworzenie sieci

VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging; automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA; przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie za pomocą RADIUS VSA np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który „przejmuje” rolę uwierzytelniania klientów; obsługa Guest VLAN dla IEEE 802.1x; możliwość przekierowania na Captive Portal podczas logowania do sieci; obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176; obsługa TACACS+ (RFC 1492); obsługa RADIUS Authentication (RFC 2865); obsługa RADIUS Accounting (RFC 2866); RADIUS per-command Authentication; obsługa RADIUS over TLS (RadSec) – RFC 6614; bezpieczeństwo MAC adresów: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresu na porcie, możliwość wpisania statycznych MAC adresów na port/vlan; możliwość wyłączenia MAC learning; zabezpieczenie przełącznika przed atakami DoS: Networks Ingress Filtering RFC 2267, SYN Attack Protection, zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania; dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4:

- adres MAC źródłowy i docelowy plus maska;
- adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6;
- protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.;
- numery portów źródłowych i docelowych TCP, UDP;
- zakresy portów źródłowych i docelowych TCP, UDP;
- identyfikator sieci VLAN – VLAN ID;
- Quality of Service IEEE 802.1p oraz DiffServ;
- flagi TCP;
- obsługa fragmentów;

dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika; możliwość konfiguracji min. 8 000 reguł na wejściu i 1000 reguł na wyjściu; możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI; obsługa bezpiecznego transferu plików SCP/SFTP; obsługa DHCP Option 82; obsługa IP Security – Trusted DHCP Server; obsługa IP Security – DHCP Snooping and Guard; obsługa IP Security – Gratuitous ARP Protection; obsługa IP Security – DHCP Secured ARP/ARP Validation; obsługa IP Security – IP Source guard; ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL; obsługa wykrywania periodycznego zaniku linku (Port-Flap); musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz

reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas; zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

f) **Bezpieczeństwo sieciowe –** przełącznik musi umożliwiać funkcję umożliwiającą statyczne skonfigurowanie portu głównego i zapasowego; w stanie normalnym, czyli bez awarii, jest używany port główny, a port zapasowy jest nieaktywny; gdy port wskazany jako główny ulegnie awarii, czyli wykryje brak połączenia (link down), to port zapasowy się automatycznie aktywuje; obsługa redundancji routingu VRRP; obsługa STP (Spanning Tree Protocol) IEEE 802.1D; obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w; obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s; obsługa PVST+; obsługa ERPS / G.8032; obsuga Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów; obsługa MLAG – połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników; obsługa LACP w ramach MLAG.

g) **Zarządzanie –** obsługa synchronizacji czasu SNTP lub NTP; zarządzanie przez SNMP v1/v2/v3; zarządzanie przez przeglądarkę WWW – protokół http i https; możliwość zarządzania przez XML API; Telnet Serwer/Klient dla IPv4 / IPv6; SSH2 Serwer/Klient dla IPv4 / IPv6; Ping dla IPv4 / IPv6; Traceroute dla IPv4 / IPv6; obsługa SYSLOG z możliwością definiowania wielu serwerów; sprzętowa obsługa sFlow; obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757); obsługa RMON2 (RFC 2021); obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS.

h) **Inne –** współpraca z oprogramowaniem zarządzającym oferowanym przez producenta przełączników; współpraca z systemem zarządzającym w chmurze oferowanym przez producenta przełączników; współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników; wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.); wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging; obsługa skryptów CLI; obsługa funkcji TCL/Tk w skryptach CLI; obsługa skryptów Python 3.x; możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych); możliwość uruchamiania skryptów – ręcznie, o określonym czasie lub co wskazany okres czasu, na podstawie wpisów w logu systemowym.

5) **<u>Przełącznik 48 portów POE+ wraz z rocznym wsparciem, kablem zasilającym i 4 kompatybilnymi wkładkami SFP 10 GB – 1 szt. – wymagania minimalne:</u>**

a) **Wymagania podstawowe:**

- Przełącznik do sieci LAN w metalowej obudowie.
- Wysokość urządzenia 1U – montaż w standardowej szafie 19".
- Głębokość urządzenia nie większa niż 35 cm.
- Przełącznik musi posiadać wbudowany zasilacz AC 230V.
- Przełącznik wyposażony w min.: 48 portów PoE+ 10/100/1000BASE-T, 8 portów SFP+ 1/10G (licencja podnosząca prędkość na 4 portach do 10G).
- Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex.
- Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet.
- Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+.
- Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów.
- PoE+ zgodne ze standardem IEEE 802.3at.

- Budżet mocy dla zasilania PoE nie mniejszy niż 740 W.
- Możliwość ustawiania priorytetów wyłączenia PoE na portach w przypadku braku mocy.
- Możliwość ustawienia włączania/wyłączania czasowego PoE.
- Wsparcie Fast PoE – uruchomienie zasilania PoE bez oczekiwania na pełne uruchomienie oprogramowania przełącznika.
- Wsparcie Perpetual PoE - brak zaniku PoE podczas restartu przełącznika.
- Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos.
- Przepustowość stosu min. 40 Gb/s.
- Możliwość budowy stosu za pomocą portów 10G SFP+.
- Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem.
- Nieblokująca architektura o wydajności przełączania min. 256 Gb/s.
- Szybkość przełączania: 190.5 Mp/s.
- Zakres temperatury pracy przełącznika: 0 - 50 stopni C.
- Pamięć operacyjna: min. 1 GB pamięci DRAM.
- Pamięć flash: min. 1 GB pamięci Flash.
- Dedykowany port konsoli szeregowej RS-232 (RJ45).
- Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika.
- Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
- Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
- Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash.
- Możliwość monitorowania zajętości CPU.
- Możliwość monitorowania zajętości pamięci.
- Wsparcie mirroringu ruchu: lokalny mirroring na przełączniku, zdalny mirroring, zdalny mirroring do wskazanego adresu IP poprzez tunel – np. GRE, możliwość mirroringu ruchu wybranego za pomocą listy kontroli dostępu ACL.
- Wsparcie diagnostyki okablowania – wykrywanie przerwy, zwarcia oraz odległości do awarii.

b) **Funkcje L2 przełącznika –** tablica MAC adresów min. 32 tys.; obsługa sieci wirtualnych IEEE 802.1Q – min. 4 tys.; obsługa funkcjonalności Private VLAN – blokowanie ruchu pomiędzy klientami z możliwieniem łączności do wspólnych zasobów sieciowych; obsługa Q-in-Q IEEE 802.1ad; wsparcie dla ramek Jumbo Frames (min. 9216 bajtów); obsługa STP (Spanning Tree Protocol) IEEE 802.1D; obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w; obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s; obsługa PVST+ (Per-VLAN Spanning Tree Protocol); obsługa min. 64 instancji MSTP; obsługa Link Aggregation IEEE 802.3ad wraz z LACP: obsługa min. 128 grup łączy typu Link Aggregation, obsługa umożliwiająca zgrupowanie min. 8 portów; obsługa MLAG (Multi Chassis Link Aggregation); obsługa protokołu EAPS – RFC 3619; obsługa

protokołu ERPS / G.8032; obsługa Quality of Service: rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p, rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym, obsługa kolejek Strict Priority, obsługa kolejek Weighted Round Robin, obsługa WRED (Weighted Random Early Detection); obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB; obsługa LLDP Media Endpoint Discovery (LLDP-MED); obsługa CDPv1 oraz CDPv2; przełącznik musi posiadać obsługę AVB (Audio Video Bridging); kontrola sztormów: możliwość ograniczenia liczby pakietów Multicast na porcie, możliwość ograniczenia liczby pakietów Broadcast na porcie, możliwość ograniczenia liczby pakietów Unknown Unicast na porcie; przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP; wsparcie DCB (Data Center Bridging): DCBX – Data Center Bridging eXchange, PFC – Priority-based Flow Control, ETS – Enhanced Transmission Selection.

c) **Funkcje L3 przełącznika IPv4 –** obsługa min. 1500 interfejsów IP; wsparcie dla IP multinetting – wiele adresów przypisanych do jednej sieci VLAN; sprzętowa obsługa routingu IPv4; pojemność sprzętowej tabeli routingu min. 12 tys. wpisów; obsługa routingu statycznego IPv4; obsługa routingu dynamicznego IPv4: RIP v1/v2, OSPFv2 min. 4 aktywne interfejsy IP – możliwość rozszerzenia do pełnej funkcjonalności przez licencję, BGPv4 min. 2 sąsiadów – możliwość rozszerzenia do pełnej funkcjonalności przez licencję, ISIS – możliwość rozszerzenia przez licencję; obsługa redundancji routingu VRRP dla IPv4; Policy Based Routing dla IPv4; obsługa DHCP Relay; obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów; obsługa Opcji 82 dla DHCP.

d) **Funkcje L3 przełącznika IPv6 –** sprzętowa obsługa routingu IPv6; pojemność tabeli routingu min. 6 tys. wpisów; obsługa routingu statycznego IPv6; obsługa routingu dynamicznego IPv6: RIPng, OSPFv3 min. 4 aktywne interfejsy IP – możliwość rozszerzenia do pełnej funkjconalności przez licencję, BGPv4 min. 2 sąsiadów – możliwość rozszerzenia do pełnej funkcjonalności przez licencję, ISIS – możliwość rozszerzenia przez licencję; obsługa redundancji routingu VRRP dla IPv6; Policy Based Routing dla IPv6; obsługa 6to4 (RFC 3056); opcja IPv6 Router Advertisement dla DNS – RFC 6106.

e) **Obsługa ruchu rozgłoszeniowego –** statyczne przyłączania portu do grupy multicast; filtrowanie IGMP; obsługa IGMP v1 – RFC 1112; obsługa IGMP v2 – RFC 2236; obsługa IGMP v3 – RFC 3376; obsługa IGMP v1/v2/v3 snooping; obsługa PIM-SM; obsługa PIM-DM – możliwość rozszerzenia przez licencję; obsługa PIM-SSM – możliwość rozszerzenia przez licencję; obsługa MLDv1 snooping; obsługa MLDv2 snooping; obsługa MVR (Multicast VLAN Registration).

f) **Funkcje bezpieczeństwa –** obsługa logowania do sieci Network Login: IEEE 802.1x based Network Login, MAC address based Network Login, Web based Network Login; obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants); obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation; przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x; przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania

do sieci MAC authentication; automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink; automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging; automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA; automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA; przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów; obsługa Guest VLAN dla IEEE 802.1x; możliwość przekierowania klienta na Captive Portal podczas logowania do sieci; obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176; obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication); obsługa RADIUS Authentication (RFC 2865); obsługa RADIUS Accounting (RFC 2866); obsługa RADIUS Per-Command Authentication – uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS; obsługa RADIUS Authentication over TLS (RadSec); obsługa RADIUS Accounting over TLS (RadSec); obsługa TACACS+ (RFC 1492); bezpieczeństwo MAC adresów: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresów na porcie, możliwość wpisania statycznych MAC adresów na port/vlan; możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning); dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4:

- adres MAC źródłowy i docelowy plus maska,
- adres IP źródłowy i docelowy plus maska dla IPv4,
- adres IP źródłowy i docelowy plus maska dla IPv6,
- protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.,
- numery portów źródłowych i docelowych TCP, UDP,
- zakresy portów źródłowych i docelowych TCP, UDP,
- identyfikator sieci VLAN – VLAN ID,
- Quality of Service IEEE 802.1p,
- Quality of Service DiffServ/DSCP,
- flagi TCP,
- obsługa fragmentów;

listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika; możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI; wsparcie 8 tys. wpisów ACL na wejściu (Ingress); wsparcie 1 tys. wpisów ACL na wyjściu (Egress); obsługa IP Security: Trused DHCP Server,

DHCP Snooping and Guard, Gratuitous ARP Protection, DHCP Secured ARP/ARP Validation, IP Source Guard; ograniczenie przepustowości (rate limiting) na portach wyjściowych; ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL; obsługa wykrywania periodycznego zaniku linku (Port-Flap): możliwość zdefniowania liczby zaniku linku w czasie określonego czasu, możliwość automatycznej reakcji polegającej na wyłączeniu portu, możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas, możliwość raportowania zdarzenia poprzez Syslog, możliwość raportowania zdarzenia poprzez Trap SNMP; możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE – GCM-AES-128; możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE – GCM-AES-256; wydajność MACSec po rozbudowie przełącznika nie mniejsza niż: 25 Gb/s.

g) **Zarządzanie –** zarządzenia przez SNMP v1/v2/v3; obsługa SNMP Traps; obsługa synchronizacji czasu SNTP lub NTP; obsługa DNS klienta; zarządzanie przez przeglądarkę www – protokół http i https; możliwość zarządzania przez protokół XML; obsługa serwera SSH dla IPv4; obsługa serwera SSH dla IPv6; obsługa klienta SSH dla IPv4; obsługa klienta SSH dla IPv6; obsługa serwera Telnet dla IPv4; obsługa serwera Telnet dla IPv6; obsługa klienta Telnet dla IPv4; obsługa klienta Telnet dla IPv6; obsługa transferu plików: TFTP, SFTP, SCP; obsługa SYSLOG; obsługa Secure SYSLOG (TLS); obsługa SYSLOG – konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń; obsługa logowania komend CLI do logu systemowego; obsługa logowania komend do serwera SYSLOG; obsługa ping dla IPv4 i IPv6; obsługa traceroute dla IPv4 i IPv6; obsługa RMON min. 4 grupy: Status, History, Alarms, Events; obsługa RMON2.

h) **Inne –** współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników; wbudowany DHCP Server; DHCP Server z możliwość definicji opcji (np. opcje 43, 60, 78 itp.); wbudowany DHCP Client; obsługa skryptów CLI; obsługa funkcji TCL/Tk w skryptach CLI; obsługa skryptów Python 3.x; możliwość uruchamiania skryptów: ręcznie z CLI przez administratora, o określonym czasie lub co wskazany czas, na podstawie zdarzeń z logu systemowego; możliwość edycji skryptów bezpośrednio na urządzeniu – system operacyjny musi zawierać edytor plików tekstowych; wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging.

i) **Zgodność z normami –** EU RoHS – 2011/65/EU; EN/ETSI 300 019-2-1 v2.1.2 – Class 1.2 Storage; EN/ETSI 300 019-2-2 v2.1.2 – Class 2.3 Transportation; EN/ETSI 300 019-2-3 v2.1.2 – Class 3.1e Operational.

j) **Gwarancja –** dożywotnia gwarancja na sprzęt – min. 5 lat po zakończeniu produkcji; dożywotnia aktualizacja oprogramowania na przełączniku.

6) **<u>System NAC – wymagania minimalne:</u>**

a) **Podstawowa funkcjonalność systemu NAC:**

- System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
- System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).

- System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
- System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
- System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
- System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
- System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
- Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
- System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
- System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: VM – min. VMWare ESXi, co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x, maszyny fizyczne – serwery wspierane przez producenta.
- System musi posiadać funkcjonalność serwerów: serwera RADIUS dla infrastruktury sieciowej, serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+, serwera SYSLOG, serwera TACACS+, serwera Monitoringu, serwera DHCP, serwera polityk uwierzytelniania i kontroli dostępu 802.1X, serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
- System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
- System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
- System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
- System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.

- Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
- System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
- System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
- System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
- System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
- System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
- System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
- Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
- System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
- System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
- System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
- System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
- System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
- Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, autoryzacji, statusu, opisu.
- System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
- System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
- System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.

- System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
- System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
- System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
- System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
- System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google, LinkedIn.
- System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
- System musi posiadać funkcję personalizacji strony gościnnej.
- Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
- Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
- Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
- Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
- Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
- Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
- Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
- Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
- Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
- Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
- Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
- System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
- System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.

- System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
- System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
- System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
- System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
- System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
- System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
- System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej: czy system jest aktualny z możliwością automatycznego naprawienia niezgodności, czy włączony jest firewall, czy jest uruchomiony system antywirusowy i aktualna baza sygnatur, czy jest włączone szyfrowanie dysku systemowego, czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory, czy na dysku znajdują się pliki lub katalogi wskazane przez administratora, czy w systemie są uruchomione procesy wskazane przez administratora, czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności, czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: wartości klucza rejestru, typu wartości: Number, String, Version.
- System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
- System musi współpracować z serwerem tokenów.
- System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej: Microsoft Windows, Mac OS, iOS, Android.
- System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
- System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

b) **Mechanizmy uwierzytelniania:**

- System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

- System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: MAC, PAP/ASCII, CHAP, SNMP, 802.1X. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
- System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
- System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
- System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
- System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: Tożsamość/Urządzenie końcowe, Grupa tożsamości/urządzeń końcowych, Parametry urządzeń końcowych, min: system operacyjny, wersja, Atrybuty Active Directory, Jednostka organizacyjna tożsamości/urządzeń końcowych, Urządzenia sieciowe sieci przewodowej, bezprzewodowej, Grupy urządzeń sieciowych, Porty urządzeń sieciowych, Grupy portów urządzeń sieciowych, Jednostka organizacyjna portów, Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), Data, czas ważności polityki, Wewnętrzny Captive Portal, Metoda autoryzacji.
- System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
- System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
- System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
- System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
- System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
- System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
- System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
- System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
- System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.

- System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
- System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
- System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
- System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

c) **Obsługa serwerów certyfikatów CA:**
- System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
- Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności: możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych; możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych; możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol); usługę OCSP (Online Certificate Status Protocol).

d) **Obsługa serwerów DHCP:**
- System musi posiadać funkcję zintegrowanego serwera DHCP.
- System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
- System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP: uruchamianie usługi dla wybranych podsieci; przypisanie ustalonego adresu IP dla adresu MAC; przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci; możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC; możliwość określania braku dostępu dla wybranych adresów MAC; monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC; możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP; możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego; możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi; dokonywanie zmian bez konieczności wyłączania usług.

e) **Obsługa serwerów TACACS+** – system musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:
- System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
- System musi umożliwiać tworzenia haseł administratorom.
- System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.

- System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
- System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
- System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
- System musi wspierać logowanie administratorów za pomocą tokenów OTP.
- System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

f) **Raportowanie i monitoring –** system musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:
- Monitoring autoryzacji.
- Monitoring dla zdarzeń systemowych.
- Monitoring dla zdarzeń DHCP.
- Monitoring dla tożsamości.
- Monitoring dla urządzeń końcowych.
- Monitoring dla urządzeń sieciowych.
- Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
- Raport ze zdarzeń logowania z informacją o nadam adresie IP.
- Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
- Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
- System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
- System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
- System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
- System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
- System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
- System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
- Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.

- Raport zdarzeń Microsoft Active Directory, minimum: logowania, wylogowania z system w tym błędne logowania, logowania do sieci 802.1X.

g) **Alarmy:**
- System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: wiadomości e-mail, Syslog, notyfikacji systemowych.
- Alarmy mogą być generowane w sytuacjach, min: ilości obsługiwanych transakcji RADIUS, opóźnienie obsługi transkacji RADIUS, statusu krytycznego modułów.
- System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: badanie łączności IP za pomocą ping, traceroute; tcpdump protokołów RADIUS, TACACS+; wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty, wykonanie zdalnego polecenia na urządzeniu sieciowym.

h) **Wymagania dotyczące wdrożenia i harmonogram ramowy:**
- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
- Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6 h dziennie.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

i) **Szkolenia/warsztaty:**
- Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC.
- Warsztaty zostaną przeprowadzone dla 2 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC.
- Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC.
- Warsztaty odbędą się na miejscu w siedzibie klienta.

- Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
- Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.

j) **Licencja wsparcia technicznego producenta oprogramowania –** Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 12 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:
- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC.
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

Wspólny Słownik Zamówień (CPV):
1) 30.20.00.00-1 – Urządzenia komputerowe;
2) 48.82.00.00-2 – Serwery;
3) 48.80.00.00-6 – Systemy i serwery informacyjne.

ROZDZIAŁ IV. TERMIN WYKONANIA ZAMÓWIENIA.
Termin wykonania zamówienia w ramach wszystkich części – 90 dni od dnia podpisania umowy.

ROZDZIAŁ V. ZAMÓWIENIA CZĘŚCIOWE ORAZ INFORMACJA O OFERCIE WARIANTOWEJ.
1. Zamawiający dopuszcza składanie ofert częściowych. Dopuszczalne jest składanie ofert zarówno na jedną jak i więcej części.
2. Zamawiający nie dopuszcza składania ofert wariantowych.

ROZDZIAŁ VI. ZAMÓWIENIA PODOBNE.
Zamawiający nie dopuszcza możliwości udzielenia zamówień polegających na powtórzeniu podobnych dostaw zgodnych z przedmiotem zamówienia podanym powyżej.

ROZDZIAŁ VII. INFORMACJA O PODWYKONAWCACH.
1. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych części zamówienia.
2. Zamawiający żąda wskazania części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez Wykonawców firm podwykonawców.
3. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby wykonawca powoływał się, na zasadach określonych w art. 118 ustawy, w celu wykazania spełniania warunków udziału w postępowaniu, wykonawca jest obowiązany wykazać zamawiającemu, że proponowany inny podwykonawca lub wykonawca

samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

ROZDZIAŁ VIII. WYKONAWCY WSPÓLNIE UBIEGAJĄCY SIĘ O ZAMÓWIENIE.

1. **Wykonawcy wspólnie ubiegający się o zamówienie:**
   - ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania;
   - muszą ustanowić Pełnomocnika Wykonawców występujących wspólnie do reprezentowania ich w postępowaniu o udzielenie zamówienia publicznego albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia. Przyjmuje się, że pełnomocnictwo do podpisania oferty obejmuje pełnomocnictwo do poświadczenia za zgodność z oryginałem wszystkich dokumentów;
   - pełnomocnictwo musi jednocześnie wynikać z umowy lub z innej czynności prawnej, mieć formę pisemną, fakt ustanowienia Pełnomocnika musi wynikać z załączonych do oferty dokumentów, wszelka korespondencja prowadzona będzie z Pełnomocnikiem;
   - przed zawarciem umowy o niniejsze zamówienie publiczne, jeżeli oferta konsorcjum zostanie wybrana jako najkorzystniejsza, Zamawiający może wezwać do przedstawienia umowy regulującej współpracę tych Wykonawców.
2. **Oferta wspólna, składana przez dwóch lub więcej Wykonawców powinna spełniać następujące wymagania:**
   1) musi być zgodna z postanowieniami SWZ;
   2) sposób składania dokumentów w przypadku składania oferty wspólnej:
      a) **dokumenty wspólne, takie jak:**
         - oferta **(Załącznik nr 1 do SWZ);**
         - minimalne wymagania techniczno – użytkowe **(Załącznik nr 2a lub 2b do SWZ);**
         - oświadczenie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO **(Załącznik nr 5 do SWZ);**

podpisują wszyscy członkowie konsorcjum lub Pełnomocnik (Lider) w imieniu całego konsorcjum.

      b) **dokumenty, takie jak:**
         - oświadczenie o spełnianiu warunków udziału w postępowaniu i braku podstaw do wykluczenia **(Załącznik nr 4 do SWZ);**

składa każdy z partnerów konsorcjum w imieniu swojej firmy.

ROZDZIAŁ IX. WYKONAWCA MAJĄCY SIEDZIBĘ LUB MIEJSCE ZAMIESZKANIA POZA TERYTORIUM RZECZYPOSPOLITEJ POLSKIEJ.

Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej składa dokumenty zgodnie z przepisami rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415).

ROZDZIAŁ X. WALUTA W JAKIEJ BĘDĄ PROWADZONE ROZLICZENIA ZWIĄZANE Z REALIZACJĄ NINIEJSZEGO ZAMÓWIENIA PUBLICZNEGO.

Wszelkie rozliczenia związane z realizacją niniejszego zamówienia dokonywane będą w walucie polskiej.

ROZDZIAŁ XI. PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy:
   1) nie podlegający wykluczeniu z postępowania na podstawie art. 108 ust 1 ustawy Pzp;
   2) nie podlegający wykluczeniu z postępowania na podstawie art. 109 ust 1 ustawy Pzp;
      a) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
      b) który naruszył obowiązki w dziedzinie ochrony środowiska, prawa socjalnego lub prawa pracy:
         – będącego osobą fizyczną skazanego prawomocnie za przestępstwo przeciwko środowisku, o którym mowa w rozdziale XXII Kodeksu karnego lub za przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, o którym mowa w rozdziale XXVIII Kodeksu karnego, lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
         – będącego osobą fizyczną prawomocnie ukaranego za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny;
         – wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z prawa ochrony środowiska, prawa pracy lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną;
      c) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo lub ukarano za wykroczenie, o którym mowa w pkt 2 lit. a lub b;
      d) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
      e) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;

f) jeżeli występuje konflikt interesów w rozumieniu art. 56 ust. 2, którego nie można skutecznie wyeliminować w inny sposób niż przez wykluczenie wykonawcy;
g) który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;
h) który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
i) który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
j) który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia.

3) nie podlegam wykluczeniu z postępowania 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. z 2022, poz. 835 z późn. zm.).

2. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2-5 i 7-10, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:
   1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
   2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
   3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
      a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
      b) zreorganizował personel,
      c) wdrożył system sprawozdawczości i kontroli,
      d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
      e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

4. Zamawiający ocenia, czy podjęte przez Wykonawcę czynności, o których mowa w ust. 3, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez Wykonawcę czynności, o których mowa w ust. 3, nie są wystarczające do wykazania jego rzetelności, Zamawiający wyklucza wykonawcę.

ROZDZIAŁ XII. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ SPOSÓB DOKONYWANIA OCENY SPEŁNIENIA TYCH WARUNKÓW.

O udzielenie zamówienia mogą ubiegać się Wykonawcy spełniający warunki udziału w postępowaniu określone w SWZ i w art. 112 ustawy Pzp:

1. **posiadający zdolności do występowania w obrocie gospodarczym, tj.:**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu;
2. **posiadający uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów, tj.:**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu;
3. **znajdujący się w sytuacji ekonomicznej lub finansowej zapewniającej prawidłowe wykonanie zamówienia, tj.:**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu;
4. **posiadający zdolności techniczne lub zawodowe zapewniającej prawidłowe wykonanie zamówienia, tj.:**
   Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu.

ROZDZIAŁ XIII. PODMIOTOWE ŚRODKI DOWODOWE.

1. Do oferty Wykonawca dołącza oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu w zakresie wskazanym przez Zamawiającego.
2. Wzór oświadczenia, o którym mowa w ust. 1 stanowi **Załącznik nr 4 do SWZ.**
3. Oświadczenie, o którym mowa w ust. 1, stanowi dowód potwierdzający brak podstaw wykluczenia, spełnianie warunków udziału w postępowaniu na dzień składania ofert, tymczasowo zastępujący wymagane przez Zamawiającego podmiotowe środki dowodowe.

4. Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia podmiotowych środków dowodowych, o których mowa w art. 273 ustawy Pzp.
5. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, podmiotowych środków dowodowych, o których mowa w art. 273 ustawy Pzp, innych dokumentów lub oświadczeń niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia, poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
6. Jeżeli wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

ROZDZIAŁ XIV. WYMAGANIA DOTYCZĄCE WADIUM.

1. Przystępując do niniejszego postępowania każdy Wykonawca zobowiązany jest wnieść **wadium w wysokości:**
   1) **Część nr 1 – 3.000,00 zł** (słownie: trzy tysiące złotych 00/100);
   2) **Część nr 2 – 2.000,00 zł** (słownie: dwa tysiące złotych 00/100).
2. Wadium można wnieść w formach przewidzianych w art. 97 ust. 7 ustawy Pzp.
3. Wykonawca zobowiązany jest wnieść wadium przed upływem terminu składania ofert.
4. Wadium w pieniądzu należy wnieść na konto Zamawiającego:

Bank Spółdzielczy Sławno Nr 50 9317 0002 0000 3131 2000 0030
z dopiskiem „Wadium na dostawę urządzeń komputerowych – Część nr ……”

5. W przypadku wadium wnoszonego w pieniądzu za termin wniesienia uznaje się chwilę uznania kwoty na rachunku Zamawiającego.
6. W przypadku wniesienia **wadium w formie innej niż pieniądz – Wykonawca przekazuje Zamawiającemu oryginał dokumentu w postaci elektronicznej.**
7. Niewniesienie wadium w terminie lub w sposób inny niż określony w SWZ skutkowało będzie odrzuceniem oferty Wykonawcy.
8. Zamawiający dokonuje zwrotu wadium zgodnie z postanowieniami art. 98 ustawy Pzp.
9. Zamawiający zwraca wadium wniesione w pieniądzu wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez Wykonawcę.
10. Zamawiający zatrzymuje wadium wraz z odsetkami w przypadkach określonych w art. 98 ustawy Pzp.

ROZDZIAŁ XV. TERMIN ZWIĄZANIA OFERTĄ.

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert **do dnia 15 sierpnia 2025 r.**
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania

ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazany przez niego okres, nie dłuższy niż 30 dni.

3. Przedłużenie terminu związania oferta, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. W przypadku gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa w ust. 2, następuje wraz z przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

ROZDZIAŁ XVI. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ.

1. W postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem https://ezamowienia.gov.pl.
2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
3. Adres strony internetowej prowadzonego postępowania (link prowadzący bezpośrednio do widoku postępowania na Platformie e-Zamówienia): https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-1f7835df-355f-4af2-99c9-1e152342f933.
4. Postępowanie można wyszukać również ze strony głównej Platformy e-Zamówienia (przycisk **„Przeglądaj postępowania/konkursy”**).
5. Identyfikator (ID) postępowania na Platformie e-Zamówienia: ocds-148610-1f7835df-355f-4af2-99c9-1e152342f933.
6. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu **„Wykonawca”** na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa **Regulamin Platformy e-Zamówienia**, dostępny na stronie internetowej https://ezamowienia.gov.pl oraz informacje zamieszczone w zakładce **„Centrum Pomocy”**.
7. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
8. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych.
9. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki. W przypadku formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, ww. regulacje nie będą miały bezpośredniego zastosowania.
10. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, przekazywane w postępowaniu sporządza się w postaci elektronicznej:

1) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik), lub
2) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści **„Formularza do komunikacji”**).

11. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913 oraz z 2021 r. poz. 1655) wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku **„Dokument stanowiący tajemnicę przedsiębiorstwa”**.
12. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce **„Formularze” („Formularze do komunikacji”)**. Za pośrednictwem **„Formularzy do komunikacji”** odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk **„dodaj załącznik”**). W przypadku załączników, które są zgodnie z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone, zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
13. Możliwość korzystania w postępowaniu z **„Formularzy do komunikacji”** w pełnym zakresie wymaga posiadania konta **„Wykonawcy”** na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z **„Formularzy do komunikacji”** służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.
14. Wszystkie wysłane i odebrane w postępowaniu przez Wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce **„Komunikacja”.**
15. Maksymalny rozmiar plików przesyłanych za pośrednictwem **„Formularzy do komunikacji”** wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
16. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa **Regulamin Platformy e-Zamówienia**.
17. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu 22 458 77 99 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce **„Zgłoś problem”.**

18. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: sekretariat@gminaslawno.pl (nie dotyczy składania ofert).
19. Zamawiający wyznacza następujące osoby do komunikowania się z Wykonawcami:
    1) Marcin Czyż (tel. 59 810 65 53).
    2) Daria Anna Dawid – Nowacka (tel. 59 810 65 71).
    3) Karolina Jurzyk (tel. 59 810 65 78).

ROZDZIAŁ XVII. INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ, W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. 69.

Zamawiający nie przewiduje komunikowania się z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej.

ROZDZIAŁ XVIII. OPIS SPOSOBU PRZYGOTOWANIA I SKŁADANIA OFERT.

1. Wykonawca składa ofertę za pośrednictwem zakładki **„Oferty/wnioski”,** widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku **„Złóż ofertę”** system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop **(„przeciągnij” i „upuść”)** służące do dodawania plików.
2. Wykonawca dodaje wybrany z dysku i uprzednio podpisany **„Formularz oferty”** w pierwszym polu **(„Wypełniony formularz oferty”).** W kolejnym polu **(„Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”)** wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
3. Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku **„Dokument stanowiący tajemnicę przedsiębiorstwa”.** Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu **„Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.**
4. **Formularz ofertowy** podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym w formacie PAdES typ wewnętrzny.
5. **Pozostałe dokumenty** wchodzące w skład oferty lub składane wraz z ofertą, które są zgodnie z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby opatrzone podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu **„Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”** dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
6. W przypadku przekazywania dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym

podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

7. System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce **„Oferty/Wnioski”.**
8. Oferta może być złożona tylko do upływu terminu składania ofert.
9. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce **„Oferty/wnioski”** używając przycisku **„Wycofaj ofertę”.**
10. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.

ROZDZIAŁ XIX. WYMÓG LUB MOŻLIWOŚĆ ZŁOŻENIA OFERT W POSTACI KATALOGÓW ELEKTRONICZNYCH LUB DOŁĄCZENIA KATALOGÓW ELEKTRONICZNYCH DO OFERTY, W SYTUACJI OKREŚLONEJ W ART. 93 USTAWY PZP

Zamawiający dopuszcza możliwość dołączenia katalogów elektronicznych do składanej oferty.

ROZDZIAŁ XX. TERMIN SKŁADANIA OFERT.

1. Ofertę wraz z wymaganymi załącznikami należy złożyć **w terminie do dnia 17 lipca 2025 roku, do godz. 09.30.**
2. Wykonawca może złożyć tylko jedną ofertę.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.

ROZDZIAŁ XXI. TERMIN OTWARCIA OFERT.

1. Otwarcie ofert nastąpi w dniu **17 lipca 2025 roku, o godz. 10.00.**
2. Niezwłocznie po otwarciu ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.

ROZDZIAŁ XXII. OPIS SPOSOBU OBLICZANIA CENY.

1. Wykonawca powinien dokonać wyceny wszystkich elementów związanych z przedmiotem zamówienia opisanym w SWZ z uwzględnieniem wszelkich kosztów, opłat i podatków zgodnie z obowiązującymi przepisami wraz z podatkiem VAT.
2. Ceny w ofercie muszą być podane do dwóch miejsc po przecinku.
3. Ceny w ofercie muszą zawierać wszystkie koszty związane z realizacją przedmiotowego zamówienia.
4. Zamawiający nie dopuszcza możliwości zmiany wynagrodzenia w okresie trwania umowy.

ROZDZIAŁ XXIII. OPIS KRYTERIÓW OCENY OFERT WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT.

Kryterium	Waga kryterium
Cena oferty	**60 %**
Termin płatności faktury (nie krótszy niż 7 dni i nie dłuższy niż 30 dni)	**40 %**
Łącznie	**100 %**

1. Maksymalna liczba punktów w danym kryterium równa jest określonej wadze kryterium w %.
2. Ocena łączna stanowi sumę punktów uzyskanych w ramach wszystkich kryteriów. Uzyskana liczba punktów zaokrąglona będzie do drugiego miejsca po przecinku.
3. Przyznawanie liczby punków poszczególnym ofertom będzie się odbywać według następujących zasad:

   1) Cena oferty.
   Ocenie zostanie poddana cena brutto oferty obliczona przez Wykonawcę zgodnie z przepisami prawa – podana w Formularzu oferty (stanowiącym Załącznik nr 1 do SWZ). Liczba punktów, którą można uzyskać w tym kryterium zostanie obliczona według wzoru:

   $$\text{liczba punktów} = \frac{\text{najniższa cena brutto spośród złożonych ofert}}{\text{cena brutto oferty ocenianej}} \times 60 \text{ pkt.}$$

   2) Termin płatności faktury.
   Termin płatności nie krótszy niż 7 dni i nie dłuższy niż 30 dni od dnia przedłożenia Zamawiającemu prawidłowo wystawionej faktury VAT. Zamawiający dokona stosownego obliczenia na podstawie wypełnionego formularza oferty (stanowiącego załącznik nr 1 do SWZ) i złożonej w nim deklaracji Wykonawcy o terminie płatności. Liczba punktów, jaką można uzyskać w tym kryterium zostanie obliczona na podstawie poniższego wzoru:

   $$\text{liczba punktów} = \frac{\text{termin płatności w ofercie ocenianej}}{\text{najdłuższy termin płatności spośród złożonych ofert}} \times 40 \text{ pkt.}$$

4. Zamówienie zostanie udzielone Wykonawcy, który uzyska najwyższą liczbę punktów w wyniku oceny oferty.
5. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
6. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybiera ofertę z najniższą ceną.
7. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa w ust. 6, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę.

8. Wykonawcy, składając oferty dodatkowe, nie mogą oferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
9. Komisja Przetargowa sprawdzi czy oferta spełnia warunki i wymogi ustawy Pzp i SWZ.
10. W toku badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
11. Na podstawie kryteriów oceny ofert Zamawiający będzie oceniał każdą spośród ofert nie podlegających odrzuceniu i wybierze ofertę najkorzystniejszą.
12. Zamawiający odrzuci ofertę, jeżeli zajdzie co najmniej jedna z przesłanek wymienionych w art. 226 ust. 1 ustawy Pzp.
13. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający informuje równocześnie Wykonawców, którzy złożyli oferty, podając uzasadnienie faktyczne i prawne, o:
    1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację;
    2) Wykonawcach, których oferty zostały odrzucone.
14. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

ROZDZIAŁ XXIV. UNIEWAŻNIENIE POSTĘPOWANIA.

1. Zamawiający unieważni postępowanie o udzielenie zamówienia w przypadkach określonych w art. 255 i 256 ustawy Pzp.
2. O unieważnieniu postępowania o udzielenie zamówienia Zamawiający zawiadamia równocześnie Wykonawców, którzy złożyli oferty podając uzasadnienie faktyczne i prawne.
3. W przypadku unieważnienia postępowania o udzielenie zamówienia z przyczyn leżących po stronie Zamawiającego, Wykonawcom, którzy złożyli oferty niepodlegające odrzuceniu, przysługuje roszczenie o zwrot uzasadnionych kosztów uczestnictwa w tym postępowaniu, w szczególności kosztów przygotowania oferty.
4. W przypadku unieważnienia postępowania o udzielenie zamówienia Zamawiający niezwłocznie zawiadamia Wykonawców, którzy ubiegali się o udzielenie zamówienia w tym postępowaniu, o wszczęciu kolejnego postępowania, które dotyczy tego samego przedmiotu zamówienia lub obejmuje ten sam przedmiot zamówienia.

ROZDZIAŁ XXV. INFORMACJE O FORMALNOŚCIACH, JAKIE ZOSTANĄ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. W zawiadomieniu o wyborze oferty najkorzystniejszej Zamawiający poinformuje Wykonawcę o terminie i miejscu zawarcia umowy.
2. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego

badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

ROZDZIAŁ XXVI. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XXVII. ISTOTNE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. Istotne postanowienia umowy zawarte zostały w projekcie umowy **Załącznik nr 3 do SWZ**.
2. Zamawiający przewiduje możliwość dokonania zmiany postanowień umowy na podstawie art. 455 ustawy Prawo zamówień publicznych, które zostaną wyrażone w formie pisemnego aneksu pod rygorem nieważności i mogą nastąpić wyłącznie w następujących sytuacjach:
   1) zmiany terminu wykonania umowy, w przypadku:
      a) wystąpienia okoliczności, których nie można było przewidzieć w chwili zawarcia umowy,
      b) wstrzymanie realizacji przedmiotu umowy przez Zamawiającego nie wynikające z przyczyn leżących po stronie Wykonawcy,
      c) wyrażenia zgody przez Zamawiającego na skrócenie terminu realizacji,
   2) w zakresie zmiany wynagrodzenia, zwłaszcza w sytuacji zmiany stawki obowiązującego podatku od towarów i usług (VAT).
3. Warunkiem dokonania zmian, o których mowa w ust. 2, jest złożenie wniosku przez stronę inicjującą zmianę zawierającego:
   1) opis propozycji zmiany,
   2) uzasadnienie zmiany,
   3) obliczenie kosztów zmiany zgodnie z zasadami określonymi w umowie, jeżeli zmiana będzie miała wpływ na wynagrodzenie Wykonawcy,
   4) opis wpływu zmiany na harmonogram realizacji i fakturowania oraz termin wykonania umowy.
4. Wykonawca nie będzie uprawniony do żądania przedłużenia terminu wykonania umowy i zwiększenia wynagrodzenia, jeżeli zmiana jest wymuszona uchybieniem czy naruszeniem umowy przez Wykonawcę – w takim przypadku koszty dodatkowe związane takimi zmianami ponosi Wykonawca.
5. Powyższe zmiany nie mogą być niekorzystne dla Zamawiającego.
6. Poza przypadkami opisanymi w niniejszym paragrafie, zmiana umowy może nastąpić w przypadkach przewidzianych w art. 455 ust. 1 pkt. 2 – 4 i ust. 2 ustawy Prawo zamówień publicznych.

ROZDZIAŁ XXVIII. INNE INFORMACJE.

Nie przewiduje się:
1) zawarcia umowy ramowej,
2) ustanowienia dynamicznego systemu zakupów,
3) wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

ROZDZIAŁ XXIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCOM.

Wykonawcom, których interes prawny w uzyskaniu zamówienia doznał lub może doznać uszczerbku w wyniku naruszenia przez Zamawiającego przepisów ustawy, przepisów wykonawczych jak też postanowień niniejszej SWZ przysługują środki ochrony prawnej przewidziane w Dziale IX (art. 505-590) ustawy Pzp.

ROZDZIAŁ XXX. INFORMACJA O OCHRONIE I PRZETWARZANIU DANYCH OSOBOWYCH.

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 ust 1-3 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. U. UE L z 2016 r. Nr 119 poz. 1 i z 2018 r. Nr 127 poz. 2), zwanym dalej „RODO” informujemy, że:

1. administratorem danych osobowych jest Gmina Sławno – Urząd Gminy Sławno, 76-100 Sławno, ul. I Pułku Ułanów 11, tel. +48 59 810 75 26,
   e-mail: sekretariat@gminaslawno.pl;
2. we wszelkich sprawach związanych z ochroną danych osobowych można kontaktować się z inspektorem danych osobowych, e-mail: odo@gminaslawno.pl, tel. 59 810 75 26 lub na adres wskazany powyżej;
3. dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego pn. **„Dostawa urządzeń komputerowych w ramach realizacji projektu – Cyberbezpieczna Gmina Sławno” ZPOP.271.22.2025**, prowadzonym w trybie przetargu nieograniczonego oraz jego realizacji;
4. dane osobowe mogą zostać przekazane / powierzone osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania przetargowego w oparciu o art. 18, 19, 74, 75 i 76 ustawy Pzp oraz podmiotom, które na mocy obowiązujących przepisów prawa mogą dokonywać oceny, weryfikacji i kontroli prowadzonego postępowania i realizacji zadania, w tym w szczególności dokumentacji związanej z pozyskiwaniem środków finansowych pochodzących z budżetu państwa i Unii Europejskiej;
5. dane osobowe nie będą przekazywane poza teren Polski / UE / Europejskiego Obszaru Gospodarczego;
6. dane osobowe będą przechowywane przez okres wynikający z obowiązujących terminów archiwizacji, w tym w szczególności w oparciu o zapisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2020 r. poz. 2320 z późn. zm.), ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164 z późn. zm.) oraz ustawy Pzp;
7. obowiązek podania danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje ich niepodania wynikają z ustawy Pzp;
8. w odniesieniu do danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, o którym mowa w art. 22 RODO;
9. osoba, której dane dotyczą ma prawo do:
   1) dostępu do danych na podstawie art. 15 RODO;
   2) sprostowania danych zgodnie z zapisami art. 16 RODO;

3) żądania ograniczenia przetwarzania danych osobowych na podstawie art. 18 RODO z wyjątkiem przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego;
− prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

10. osoba, której dane dotyczą nie ma prawa do:
    1) usunięcia danych osobowych w związku z art. 17 ust. 3 lit. B, d i e RODO;
    2) przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
    3) sprzeciwu, wobec przetwarzania danych osobowych na podstawie art. 21 RODO, gdyż podstawą przetwarzania danych jest art. 6 ust. 1 lit. c i e RODO.

UWAGI:

Informacja o Finansowaniu

Niniejsze zamówienie współfinansowane jest w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.

Załącznik nr 1 do SWZ

FORMULARZ OFERTY

Gmina Sławno
ul. I Pułku Ułanów 11
76-100 Sławno

Odpowiadając na ogłoszenie dotyczące zamówienia pn.: **„Dostawa urządzeń komputerowych w ramach realizacji projektu – Cyberbezpieczna Gmina Sławno”** oferujemy wykonanie przedmiotu zamówienia zgodnie z wymogami zawartymi w Specyfikacji Warunków Zamówienia za cenę:

Cześć nr 1
wartość netto zamówienia: …….. zł,
VAT - …….. %: …….… zł,
wartość brutto zamówienia: …….. zł,
słownie: ……
w tym:

Nazwa	Cena jednostkowa	podatek VAT		Cena jednostkowa	Ilość sztuk	Wartość całkowita	Wartość całkowita
	netto	%	zł	brutto		netto	brutto
Serwery wraz z macierzą dyskową					1		
Karta sieciowa do obecnego serwera					1		
Oprogramowanie					6		
Wdrożenie oprogramowania, uruchomienie, instalacja i konfiguracja serwerów, macierzy dyskowej					1		
Zasilacz awaryjny serwerowy					2		
Zasilacz awaryjny					13		

Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.

Termin płatności faktury: ……dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Cześć nr 2
wartość netto zamówienia: …….. zł,
VAT - …….. %: ……..… zł,
wartość brutto zamówienia: …….. zł,
słownie: ……
w tym:

Nazwa	Cena jednostkowa	podatek VAT		Cena jednostkowa	Ilość sztuk	Wartość całkowita	Wartość całkowita
	netto	%	zł	brutto		netto	brutto
Rozszerzenie obecnego UTM o funkcję HA					1		
Wdrożenie rozszerzenia obecnego UTM o funkcję HA					1		
System bezpiecznego zdalnego dostępu					1		
Wdrożenie sytemu bezpiecznego zdalnego dostępu					1		
System do kontroli poczty elektronicznej					1		
Przełącznik sieciowy					2		
Przełącznik sieciowy POE					1		
Dostawa NAC					1		
Wdrożenia i konfiguracja NAC					1		

Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.

Termin płatności faktury: ……dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Nazwa i adres podmiotu składającego ofertę:
.....
NIP ..... REGON .....

Adres, na który Zamawiający powinien przesyłać ewentualną korespondencję (skrytka e-PUAP): .....
Osoba wyznaczona do kontaktów z Zamawiającym:
.....
Numer telefonu: .....
Numer faksu: .....
e-mail .....

1. Oświadczam, że podmiot, który reprezentuję to (zaznaczyć właściwe):
   □ mikroprzedsiębiorstwo,
   □ małe przedsiębiorstwo,
   □ średnie przedsiębiorstwo,
   □ jednoosobowa działalność gospodarcza,
   □ osoba fizyczna nieprowadząca działalności gospodarczej,
   □ inny rodzaj.
2. Oświadczamy, że:
   1) zapoznaliśmy się z warunkami podanymi przez Zamawiającego w SWZ i nie wnosimy do nich żadnych zastrzeżeń,
   2) uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia.
   3) akceptujemy istotne postanowienia umowy oraz termin realizacji przedmiotu zamówienia podany przez Zamawiającego,
   4) uważamy się za związanych niniejszą ofertą od dnia upływu terminu składania ofert do dnia wskazanego w Rozdziale XV ust. 1.
3. W przypadku udzielenia nam zamówienia zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
4. Oferta została złożona na …….. stronach.
5. Do oferty dołączono:

➢ Minimalne wymagania techniczno – użytkowe – Załącznik nr ……. (2a lub 2b) do SWZ.
➢Oświadczenie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO.
➢……,
➢……,
➢……,
➢……,

....., dn. .....

.....
Podpis/-y osób uprawnionych do składania świadczeń woli w imieniu Wykonawcy oraz pieczątka imienna / pieczątki

Załącznik nr 2a do SWZ

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

CZĘŚĆ NR 1 – DOSTAWA SERWERÓW, MACIERZY PAMIĘCI MASOWEJ, SYSTEMÓW OPERACYJNYCH WRAZ Z USŁUGAMI ORAZ ZASILACZY AWARYJNYCH

Serwer – 2 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Obudowa	● Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5” ● Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. ● Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.	
Płyta główna	● Płyta główna z możliwością zainstalowania do dwóch procesorów. ● Obsługa procesorów 32 rdzeniowych. ● Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. ● Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. ● Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	
Procesor	Zainstalowane dwa procesory 12-rdzeniowe, min. 2.4 GHz (częstotliwość bazowa), klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 239 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	
RAM	Minimum 256 GB DDR5 RDIMM 5600MT/s w kościach 64GB	
Gniazda PCI	Minimum dwa sloty PCIe generacji 5	
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10.	
Dyski twarde	● Zainstalowane 2 x dysk SSD SATA o pojemności min. 480 GB, 6Gb, 2,5“ Hot-Plug. ● Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.	
Interfejsy	● Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w	

sieciowe/FC/SAS	standardzie BaseT ● 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) ● 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 ● W zestawie z serwerem muszą znajdować się 2 kable DAC 10GbE SFP+/SFP+ min. 3m, dostarczone przez producenta serwera ● W zestawie z serwerem wykonawca dostarczy 3 patchcordy RJ-45 cat 6 o długości minimum 3m	
Elementy montażowe	● Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych ● Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych	
Wbudowane porty	4 porty USB w tym min: ● 1 port USB 3.0 z tyłu obudowy, ● 1 port micro USB z przodu obudowy, ● 2 port VGA z czego jeden z przodu obudowy, ● Możliwość rozbudowy o port RS232	
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200	
Zasilacze	Redundantne, Hot-Plug min. 1100 W klasy Titanium	
System operacyjny / dodatkowe oprogramowanie	Fabrycznie zainstalowany system operacyjny Microsoft Windows Serwer 2025 Standard: ● Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. ● Dostarczona z serwem licencja musi uprawniać do uruchomienia w środowisku wirtualnym co najmniej sześciu systemów Windows Server 2025 ● Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. Dodatkowe licencje: ● Serwery muszą zostać dostarczone z licencjami CAL dostarczonymi przez producenta oferowanych serwerów - łącznie 50 licencji na użytkownika Windows Server 2025 (Windows Server 2025 User CAL)	
Bezpieczeństwo	● Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. ● Możliwość wyłączenia w BIOS funkcji przycisku zasilania. ● BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła ● Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. ● Moduł TPM 2.0 ● Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera ● Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu	

	operacyjnego, uruchamiane z poziomu zarządzania serwerem ● Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). ● Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ● zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ● zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ● szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ● możliwość podmontowania zdalnych wirtualnych napędów; ● wirtualną konsolę z dostępem do myszy, klawiatury; ● wsparcie dla IPv6; ● wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ● możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ● możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ● integracja z Active Directory; ● możliwość obsługi przez dwóch administratorów jednocześnie; ● wsparcie dla automatycznej rejestracji DNS; ● wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ● możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ● możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera ● z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze	

	○ Automatyczna rejestracja certyfikatów (ACE)	
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ● Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ● integracja z Active Directory ● Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ● Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ● Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ● Szczegółowy opis wykrytych systemów oraz ich komponentów ● Możliwość eksportu raportu do CSV, HTML, XLS, PDF ● Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ● Grupowanie urządzeń w oparciu o kryteria użytkownika ● Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ● Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ● Szybki podgląd stanu środowiska ● Podsumowanie stanu dla każdego urządzenia ● Szczegółowy status urządzenia/elementu/komponentu ● Generowanie alertów przy zmianie stanu urządzenia. ● Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ● Integracja z service desk producenta dostarczonej platformy sprzętowej ● Możliwość przejęcia zdalnego pulpitu ● Możliwość podmontowania wirtualnego napędu ● Kreator umożliwiający dostosowanie akcji dla wybranych alertów ● Możliwość importu plików MIB ● Przesyłanie alertów „as-is” do innych konsol firm trzecich ● Możliwość definiowania ról administratorów ● Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ● Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ● Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ● Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ● Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o	

	stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ● Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ● Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ● Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ● Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ● Zdalne uruchamianie diagnostyki serwera. ● Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ● Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.	
Certyfikaty	● Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 ● Serwer musi posiadać deklaracja CE. ● Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** ● Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.	
Dokumentacja użytkownika	● Zamawiający wymaga dokumentacji w języku polskim lub angielskim. ● Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
Warunki	● Zamawiający wymaga zapewnienia gwarancji Producenta z	

gwarancji	zakresu wdrażanej technologii na okres 7 lat. ● Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. ● Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. ● Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. ● Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. ● Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. ● Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. ● Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. ● Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący	

	się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.	

Dodatkowa karta dla posiadanego serwera – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Karta sieciowa	• Należy dostarczyć nową kartę sieciową dwuportową 25Gb SFP28 niskoprofilową, zatwierdzoną do pracy w serwerze Dell R550 przez producenta tego serwera. • Karta musi pochodzić z autoryzowanej dystrybucji producenta serwera.	

Macierz – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5”	
Przestrzeń dyskowa	Zainstalowane: • 11 x dysk SSD SAS o pojemności min. 1.92 TB, • Hot-Plug, • 1 DWPD	
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.	
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej.	

Sposób zabezpieczenia danych	• Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). • Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. • Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). • Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.	
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.	
Pamięć cache	• Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. • Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. • Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.	
Rozbudowa pamięci cache	• Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. • Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.	
Interfejsy	• Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI w standardzie SFP28 (4 porty na kontroler). • W zestawie musi znajdować się 6 kabli DAC 25GbE SFP28/SFP28 min. 3m, dostarczonych przez producenta macierzy.	
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.	
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	• Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. • Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-	

	striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
Thin Provisioning	• Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. • Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
Tiering	• Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. • Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. • Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.	
Wewnętrzne kopie migawkowe	• Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. • Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
Wewnętrzne kopie pełne	• Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez	

	macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.	
Zdalna replikacja danych	• Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. • Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.	
Podłączanie zewnętrznych systemów operacyjnych	• Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). • Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. • Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.	
Redundancja	• Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. • Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. • Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. • Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.	
Dodatkowe wymagania	• Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.	

	• Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.	
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: • EN 62368-1 (European Union), • IEC 60950-1 (International).	
Inne	• Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. • Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. • Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. • Deklaracja zgodności CE.	
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty	

	potwierdzające należy załączyć do oferty.	

<u>Wdrożenie oprogramowania, uruchomienie, instalacja i konfiguracja serwerów, macierzy dyskowej – 1 kpl.:</u>

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Wdrożenie oprogramowania, uruchomienie, instalacja i konfiguracja serwerów, macierzy dyskowej	• Usługa wdrożenia musi obejmować montaż dostarczonej karty sieciowej w posiadanym przez zamawiającego serwerze Dell R550. • Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego, a także odpowiednie redundantne połączenie oferowanych serwerów z macierzą. • Na oferowanych urządzeniach musi zostać przeprowadzona aktualizacja firmware'u. Urządzenia zostaną skonfigurowane zgodnie z najlepszymi praktykami (w tym zasób dyskowy na macierzy dla podłączonych serwerów), a na oferowanych serwerach zainstalowane zostanie oprogramowanie do wirtualizacji (Windows Server Hyper-V) wraz z obsługą klastra trybu failover. • Przy wykorzystaniu zaoferowanych licencji Microsoft muszą zostać utworzone nowe maszyny wirtualne z systemem Windows Server 2025 Standard. Maszyny należy uruchomić w ramach klastra trybu failover. • Wszystkie wymienione prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym. • Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów. • Wykonawca powinien posiadać certyfikaty z firm, których rozwiązania wdraża.	

Zasilacz awaryjny serwerowy – 2 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej niż 3000VA / 2700W • Wersja do montażu w szafie Rack – szyny montażowe w zestawie • Technologia Podwójnej konwersji (online) • Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Wysokość n.p.m. podczas pracy 0-3000 m • Rozpraszanie ciepła w trybie online ≤703,00 BTU/h • Sprawność:	

	○ Klasa ochrony IP 20 ○ Klasa energetyczna sprzętu przeciwprzepięciowego 340J	
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Częstotliwość wejściowa 40–70 Hz • Typ gniazda wejściowego: IEC-320 C20, • Zmienny zakres napięcia wejściowego w trybie podstawowym (pełne obciążenie) 160 – 275 V; (połowa obciążenia) 100 – 275V	
Parametry wyjściowe	• Napięcie wyjściowe 230V • Częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz ±3Hz • Inne napięcia wyjściowe 220, 240 V (nastawa z wyświetlacza) • Współczynnik szczytu 3:1 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe: ○ 8 szt. IEC 320 C13 ○ 2 szt. IEC 320 C19 • Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)	
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny • Czas autonomii: ○ 3 minuty 58 sekund dla pełnego obciążenia ○ 11 minut 48 sekund dla połowy obciążenia • Typowy czas ładowania 3 godziny • Oczekiwana żywotność akumulatora (lata) 3 – 5 • Baterie wymieniane na gorąco • Możliwość rozszerzenia czasu podtrzymania poprzez dodanie do 10 zewnętrznych modułów akumulatorowych	
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 (Zasilacz dostarczany wraz z kartą zarządzania sieciowego) • Porty komunikacyjne: serial (RJ-45), Smart-Slot, USB (typ A) • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Awaryjny wyłącznik zasilania (EPO)	
Certyfikaty, zgodności oraz gwarancja	• CE, EN/IEC 62040-1, EN/IEC 62040-2, VDE, RoHS, REACh • 3 lata gwarancji producenta door to door na naprawy lub wymiany w krajach Unii Europejskiej	
Oprogramowanie	Dostępne oprogramowanie do zarządzania/monitoringu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.	

Zasilacz awaryjny – 13 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej niż 540W / 900VA • Topologia line-interactive • Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Klasa energetyczna sprzętu przeciwprzepięciowego 613 J • Automatyczna regulacja napięcia (AVR)	
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Zakres napięcia wejściowego 176 - 294 V • Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) • Standard wtyczki: CEE 7/7P	

Parametry wyjściowe	• Napięcie wyjściowe 230V
	• Częstotliwość na wyjściu 50/60Hz +/- 1 Hz
	• Typ przebiegu: Schodkowa aproksymacja sinusoidy
	• RJ11 zabezpiecznie przeciwprzepięciowe sieci fax/tel
	• Złącza/gniazda wyjściowe:
	  ○ 3 gniazda Francuskie z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania,
	  ○ 3 gniazda Francuskie z zabezpieczeniem przeciwprzepięciowym	

Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu
	• Czas autonomii:
	  ○ 4 minuty 38 sekund dla pełnego obciążenia
	  ○ 16 minut 18 sekund dla połowy obciążenia
	• Typowy czas ładowania 8 godzin
	• Oczekiwana żywotność akumulatora (lata) 3 – 5
	• Baterie wymieniane na gorąco	

Komunikacja i zarządzanie	• Gniazda RJ45 (Gigabit), USB&Serial • Ekran LCD informujący o statusie pracy oraz poziomie naładowania akumulatorów. • Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, wykrycie wymiany akumulatora	
Certyfikaty, zgodności oraz gwarancja	• CE, RoHS, REACh • 3 lata gwarancji producenta door to door na naprawy lub wymiany w krajach Unii Europejskiej	

Oprogramowanie	Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące: • Monitorowania i zarządzania zasilaczy UPS • Bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem • Bezpieczny dostęp do internetowego interfejsu użytkownika (UI) • Możliwość dokładnego określania czasu i sekwencji wyłączania za pomocą dziennika zdarzeń • Identyfikacja potencjalnych zagrożeń, możliwość eksportowania dziennika zdarzeń	

....., dn. .....

.....
Podpis/-y osób uprawnionych do składania świadczeń woli w imieniu Wykonawcy oraz pieczątka imienna / pieczątki

Załącznik nr 2b do SWZ

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

CZĘŚĆ NR 2 – ROZSZERZENIE OBECNEGO UTM O FUNKCJĘ HA WRAZ Z WDROŻENIEM, DOSTAWA SYSTEMU BEZPIECZNEGO ZDALNEGO DOSTĘPU WRAZ Z WDROŻENIEM, SYSTEMU DO KONTROLI POCZTY ELEKTRONICZNEJ WRAZ Z WDROŻENIEM. DOSTAWA PRZEŁĄCZNIKÓW SIECIOWYCH. DOSTAWA, WDROŻENIE I KONFIGURACJA NAC

Urządzenie HA do obecnego urządzenia UTM z systemem montażu umożliwiającym mocowanie w szafie serwerowej:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Urządzenie HA	Dostawa dodatkowego urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym Sonicwall TZ570; urządzenie standby powinno mieć identyczne parametry wydajnościowe oraz sprzętowe jak podstawowa jednostka; urządzenia powinny synchronizować pomiędzy sobą stany sesji połączeń; obecne urządzenie to Sonicwall TZ570; uruchomienie systemu HA; weryfikacja reguł na obecnym urządzeniu UTM.	

System bezpiecznego zdalnego dostępu:

Producent	
Nazwa	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
System bezpiecznego zdalnego dostępu	– Licencja wieczysta na oprogramowanie do bezpiecznego zdalnego dostępu z interfejsem graficznym jednolitym z urządzeniem UTM. – Zapewniające równoczesny zdalny dostęp 15 osobom. – Oprogramowanie musi posiadać wsparcie producenta do 30.06.2026 r. – Wdrożenie.	

System do kontroli poczty elektronicznej:

Producent	
Nazwa	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Wymagania ogólne	– System ochrony poczty musi działać w środowisku hostowanym poza infrastrukturą klienta na terenie Unii Europejskiej. – System powinien funkcjonować jako Proxy ze wsparciem dla protokołu SMTP. – System powinien posiadać własne filtry reputacji oraz mechanizmy antyphishingowe oraz antyspamowe. – System powinien umożliwiać skanowanie przychodzącej i wychodzącej. – Możliwość wykorzystania rekordów SPF oraz mechanizmu DKIM oraz DMARC. – Automatyczna aktualizacja filtrów bez przerywania pracy. – Musi posiadać wewnętrzną konsolę do administrowania (Web), bez potrzeby instalowania klientów. – Możliwość stworzenia kwarantanny per użytkownik. Umożliwianie użytkownikowi zarządzania własną kwarantanną, usuwanie wiadomości lub zwolnienie tych, które nie uważają za SPAM, a także możliwość blokowania e-maili. Kwarantanna może być implementowana z bezpośrednią integracją z aplikacji poczty e-mail lub przez interfejs WWW (HTTPS). – Możliwość uruchomienia konsoli web, dzięki której użytkownicy mogą sprawdzać wiadomości, które są poddawane kwarantannie ze względu na spam. – Możliwość, aby użytkownicy sami tworzyli listy wyjątków dla nadawców w konsoli web. – Umożliwianie użytkownikom na przeglądanie podejrzanych wiadomości w kwarantannie i zaakceptowanie nadawców bez interwencji administratora. – Umożliwianie użytkownikowi na utworzenie osobistych, białych list (zaufanych adresów), niezależnie od administratora, tak aby te białe listy nie kolidowały z filtrami innych użytkowników. – Moduł kwarantannowy powinien znajdować się w samym systemie antyspamowym i być w stanie wysłać okresowe powiadomienie do użytkowników, informując o wiadomościach traktowanych jako SPAM, które zostały wstawione do kwarantanny. – Użytkownik powinien być w stanie automatycznie usunąć wiadomości poddane kwarantannie zgodnie z ustawieniami określonymi przez administratora. – System powinien dawać możliwość powiadomienia administratora pocztą e-mail, jeśli filtry antyspamowe nie otrzymują aktualizacji przez pewien czas. Przyjmuje się alternatywnie, że administrator zostanie powiadomiony w przypadku błędów aktualizacji. – Rozwiązanie powinno być w stanie tworzyć i zarządzać wieloma grupami użytkowników i definiować zróżnicowane	

	reguły i polityki dla każdej z tych grup. System powinien integrować się z bazą LDAP. – Rozwiązanie umożliwia stosowanie filtrów, które aplikowane są przed wejściem wiadomości do systemu. Filtry te muszą mieć możliwość klasyfikacji różnych typów zachowań (takich jak białe i czarne listy). Filtry połączeń muszą być konfigurowane przynajmniej przez: adres IP; zakres adresów IP; muszą wspierać RBL (listy oparte o DNS); muszą posiadać i mieć możliwość używania filtrów reputacji; muszą być w stanie definiować następujące polityki: limit ilości odbiorców na wiadomość, limit wielkości wiadomości; pozwalać lub zabraniać używania SSL/ TSL dla połączeń; używać antyspam; musi wpierać SSL / TLS dla połączeń przychodzących i wychodzących; musi mieć możliwość używania odwrotną translację adresów DNS (revDNS); urządzanie powinno wspierać wiele domen (rekordów MX). – Kolejki dostarczania w oprogramowaniu MTA muszą być na tyle duże, aby wspierać przeładowanie wiadomościami w sytuacji awarii albo problemów w innych punktach infrastruktury pocztowej. – Rozwiązanie powinno wspierać unikalne profile, które obsługują zachowanie wiadomości odbijanych bazując na domenach lub na docelowych adresach IP. – Moduł kwarantanny powinien być w stanie wysłać okresowe powiadomienie dla użytkowników, informując o wiadomościach traktowanych jako spam, które zostały przeniesione do kwarantanny. – Directory Collection Protection: rozwiązanie musi posiadać ochronę przed tego typu atakami dzięki skanowaniu odbiorcy wiadomości w LDAP, Active Directory. – DoS: system operacyjny urządzenia fizycznego lub wirtualnego powinien mieć możliwość identyfikacji i ochrony MTA przed atakami typu DoS. – System uwierzytelniania powinien mieć ochronę przed atakami (np. atak słownikowy). – Posiadać funkcję zapory e-mail, chroniąc serwer poczty przed atakiem typu Directory Harvest Attack (DHA). – Filtry ochrony przed spamem powinny skanować wszystkie części wiadomości, w tym: nadawcy (komenda SMTP MAIL FROM), odbiorcy (komenda SMTP RCPT TO), nagłówek wiadomości, treść wiadomości e-mail, załączniki widomości e-mail. – Filtry bezpieczeństwa: urządzenie musi posiadać mechanizm identyfikacji treści wiadomości takich elementów jak: numer karty kredytowej, RG i / lub CPF; musi posiadać mechanizmy tworzenia katalogów słów należących do konkretnych tematów, takich jak przestępstwa; musi zezwalać na heurystyczną weryfikację nowo wprowadzonych wirusów, nawet bez dostępnej szczepionki; musi pozwalać na weryfikację rzeczywistego typu pliku	

	nawet po zmianie nazwy; umożliwiać skanowanie plików wykonywalnych skompresowanych; posiadać ochronę przed oprogramowaniem szpiegującym bez potrzeby dodatkowego oprogramowania lub agenta; ochrona przed Dialerami bez potrzeby dodatkowego oprogramowania lub agenta. – Rozwiązanie powinno umożliwiać wysyłanie plików do dodatkowej analizy w systemie sandbox przy czym system sandbox powinien posiadać co najmniej cztery równolegle działające silniki w tym dwa pochodzące od innego producenta. – System powinien umożliwiać weryfikację linków zawartych w wiadomościach nawet po dostarczeniu wiadomości do adresata. – System powinien umożliwiać zablokowanie załączniku których zaszyfrowanych hasłem. – System powinien umożliwiać wykonanie akcji na wiadomościach takich jak: przesłanie do JunkBox; otagowanie tematu; dodatnie zdefiniowanego przez administratora nagłówka; usunięcie dowolnego nagłówka; dodanie tekstu do wiadomości; odrzucenie wiadomości; przekierowanie wiadomości do innego serwera IP; pominięcie skanowania Sanbox-a.	
Licencje	– System powinien zostać dostarczony w licencjami do ochrony 50 skrzynek pocztowych. – Licencje powinny zapewniać ochronę antyspam, antyphising, antywirus, sandboxing oraz wsparcie techniczne 24x7 ora na okres do 30.06.2026 r. – System powinien posiadać jednolity interfejs z obecnym rozwiązaniem do ochrony styku lokalnej sieci z Internetem.	
Wdrożenie		

Przełącznik 48 portów wraz z rocznym wsparciem, kablem zasilającym i 4 kompatybilnymi wkładkami SFP 10 GB – 2 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Wymagania podstawowe	– Przełącznik wyposażony w 48 portów 10/100/1000BASE-T. – Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex. – Przełącznik musi być wyposażony w 8 portów uplink SFP+ 1/10G. Jeśli do pracy w trybie 10G wymagana jest licencja, to musi być ona dostarczona. – Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet. – Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów.	

	– Wszystkie porty przełącznika muszą mieć możliwość wsparcia szyfracji MACsec 128/256-bit. Jeśli funkcjonalność wymaga dodatkowej licencji, to nie musi być ona dostarczona. – Wysokość urządzenia 1U montowana w standardowym 19” Rack. – Przełącznik musi posiadać wbudowany zasilacz 230V. – Przełącznik musi posiadać możliwość łączenia z innymi przełącznikami w stos z wydajnością min. 40 Gb/s. – Przełącznik musi umożliwiać stworzenie stosu złożonego z 8 przełączników. – Stos musi zachowywać się jak jedno urządzenie logiczne, a w szczególności mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem. – Porty przełącznika, używane do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty transmisji danych SFP+ z przepustowością 10 Gb/s. – Nieblokująca architektura o wydajności przełączania min. 256 Gb/s. – Szybkość przełączania min. 190 Milionów pakietów na sekundę. – Temperatura pracy przełącznika w zakresie min. 0^{o} do 50^{o} C. – Tablica MAC adresów min. 32 tys. – Pamięć operacyjna: min. 1 GB pamięci DRAM. – Pamięć flash: min. 1 GB pamięci Flash. – Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094. – Obsługa funkcjonalności Private VLAN – blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci. – Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów). – Obsługa Q-in-Q IEEE 802.1ad. – Obsługa Quality of Service: rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p; rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ; 8 kolejek priorytetów na każdym porcie wyjściowym; obsługa kolejek Strict Priority; obsługa kolejek Weighted Round Robin; obsługa WRED (Weighted Random Early Detection). – Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB. – Obsługa LLDP Media Endpoint Discovery (LLDP-MED). – Obsługa CDPv2. – Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. – Możliwość instalacji min. dwóch wersji oprogramowania – firmware. – Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash.	

	– Możliwość monitorowania zajętości CPU oraz pamięci. – Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring). – Obsługa Wirtualnych Routerów – możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach. – Dedykowany port konsoli szeregowej RJ45. – Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika.	
Obsługa Routingu IPv4	Sprzętowa obsługa routingu IPv4 – forwarding; pojemność sprzętowej tabeli routingu min. 8 000 wpisów; routing statyczny; obsługa routingu dynamicznego IPv4: RIP v1/v2, OSPFv2 – możliwość rozszerzenia przez licencje, BGPv4 – możliwość rozszerzenia przez licencje, IS-IS – możliwość rozszerzenia przez licencje; Policy Based Routing dla IPv4; obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów.	
Obsługa Routingu IPv6	Sprzętowa obsługa routingu IPv6 – forwarding; pojemność tabeli routingu min. 4 000 wpisów; routing statyczny; obsługa routingu dynamicznego dla IPv6: RIPng, OSPF v3 – możliwość rozszerzenia przez licencje, BGPv4 – możliwość rozszerzenia przez licencje, IS-IS – możliwość rozszerzenia przez licencje; obsługa 6to4 (RFC 3056); obsługa MLDv1 (Multicast Listener Discovery version 1); obsługa MLDv2 (Multicast Listener Discovery version 2); Policy Based Routing dla IPv6; opcja IPv6 Router Advertisement dla DNS – RFC 6106.	
Obsługa Multicastów	Statyczne przyłączanie do grupy multicast; filtrowanie IGMP; obsługa PIM-SM; obsługa PIM-DM – możliwość rozszerzenia przez licencje; obsługa PIM-SSM – możliwość rozszerzenia przez licencje; obsługa Multicast VLAN Registration – MVR; obsługa IGMP v1 – RFC 1112; obsługa IGMP v2 – RFC 2236; obsługa IGMP v3 – RFC 3376; obsługa IGMP v1/v2/v3 snooping; możliwość konfiguracji statycznych tras dla Routingu Multicastów.	
Bezpieczeństwo	Obsługa logowania do sieci Network Login: IEEE 802.1x based Network Login, MAC based Network Login, Web-based Network Login; obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants); obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation; przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication – RFC 3580; automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging; automatyczne włączenie DHCP snooping oraz ARP	

	Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA; przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie za pomocą RADIUS VSA np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który „przejmuje” rolę uwierzytelniania klientów; obsługa Guest VLAN dla IEEE 802.1x; możliwość przekierowania na Captive Portal podczas logowania do sieci; obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176; obsługa TACACS+ (RFC 1492); obsługa RADIUS Authentication (RFC 2865); obsługa RADIUS Accounting (RFC 2866); RADIUS per-command Authentication; obsługa RADIUS over TLS (RadSec) – RFC 6614; bezpieczeństwo MAC adresów: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresu na porcie, możliwość wpisania statycznych MAC adresów na port/vlan; możliwość wyłączenia MAC learning; zabezpieczenie przełącznika przed atakami DoS: Networks Ingress Filtering RFC 2267, SYN Attack Protection, zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania; dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4: – adres MAC źródłowy i docelowy plus maska; – adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6; – protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.; – numery portów źródłowych i docelowych TCP, UDP; – zakresy portów źródłowych i docelowych TCP, UDP; – identyfikator sieci VLAN – VLAN ID; – Quality of Service IEEE 802.1p oraz DiffServ; – flagi TCP; – obsługa fragmentów; dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika; możliwość konfiguracji min. 8 000 reguł na wejściu i 1000 reguł na wyjściu; możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI; obsługa bezpiecznego transferu plików SCP/SFTP; obsługa DHCP Option 82; obsługa IP Security – Trusted DHCP Server; obsługa IP Security – DHCP Snooping and Guard; obsługa IP Security – Gratuitous ARP Protection; obsługa IP Security – DHCP Secured ARP/ARP Validation; obsługa IP Security – IP Source guard; ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL; obsługa wykrywania periodycznego zaniku linku (Port-Flap); musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas; zdarzenie musi	

	być raportowane poprzez Trap SNMP i/lub Syslog.	
Bezpieczeństwo sieciowe	Przełącznik musi umożliwiać funkcję umożliwiającą statyczne skonfigurowanie portu głównego i zapasowego; w stanie normalnym, czyli bez awarii, jest używany port główny, a port zapasowy jest nieaktywny; gdy port wskazany jako główny ulegnie awarii, czyli wykryje brak połączenia (link down), to port zapasowy się automatycznie aktywuje; obsługa redundancji routingu VRRP; obsługa STP (Spanning Tree Protocol) IEEE 802.1D; obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w; obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s; obsługa PVST+; obsługa ERPS / G.8032; obsuga Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów; obsługa MLAG – połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników; obsługa LACP w ramach MLA.	
Zarządzanie	Obsługa synchronizacji czasu SNTP lub NTP; zarządzanie przez SNMP v1/v2/v3; zarządzanie przez przeglądarkę WWW – protokół http i https; możliwość zarządzania przez XML API; Telnet Serwer/Klient dla IPv4 / IPv6; SSH2 Serwer/Klient dla IPv4 / IPv6; Ping dla IPv4 / IPv6; Traceroute dla IPv4 / IPv6; obsługa SYSLOG z możliwością definiowania wielu serwerów; sprzętowa obsługa sFlow; obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757); obsługa RMON2 (RFC 2021); obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS.	
Inne	Współpraca z oprogramowaniem zarządzającym oferowanym przez producenta przełączników; współpraca z systemem zarządzającym w chmurze oferowanym przez producenta przełączników; współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników; wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.); wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging; obsługa skryptów CLI; obsługa funkcji TCL/Tk w skryptach CLI; obsługa skryptów Python 3.x; możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych); możliwość uruchamiania skryptów – ręcznie, o określonym czasie lub co wskazany okres czasu, na podstawie wpisów w logu systemowym.	

Przełącznik 48 portów POE+ wraz z rocznym wsparciem, kablem zasilającym i 4 kompatybilnymi wkładkami SFP 10 GB – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie

Wymagania podstawowe	– Przełącznik do sieci LAN w metalowej obudowie. – Wysokość urządzenia 1U – montaż w standardowej szafie 19". – Głębokość urządzenia nie większa niż 35 cm. – Przełącznik musi posiadać wbudowany zasilacz AC 230V. – Przełącznik wyposażony w min.: 48 portów PoE+ 10/100/1000BASE-T, 8 portów SFP+ 1/10G (licencja podnosząca prędkość na 4 portach do 10G). – Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex. – Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet. – Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+. – Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów. – PoE+ zgodne ze standardem IEEE 802.3at. – Budżet mocy dla zasilania PoE nie mniejszy niż 740 W. – Możliwość ustawiania priorytetów wyłączenia PoE na portach w przypadku braku mocy. – Możliwość ustawienia włączania/wyłączania czasowego PoE. – Wsparcie Fast PoE – uruchomienie zasilania PoE bez oczekiwania na pełne uruchomienie oprogramowania przełącznika. – Wsparcie Perpetual PoE - brak zaniku PoE podczas restartu przełącznika. – Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos. – Przepustowość stosu min. 40 Gb/s. – Możliwość budowy stosu za pomocą portów 10G SFP+. – Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem. – Nieblokująca architektura o wydajności przełączania min. 256 Gb/s. – Szybkość przełączania: 190.5 Mp/s. – Zakres temperatury pracy przełącznika: 0 - 50 stopni C. – Pamięć operacyjna: min. 1 GB pamięci DRAM. – Pamięć flash: min. 1 GB pamięci Flash. – Dedykowany port konsoli szeregowej RS-232 (RJ45). – Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika. – Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. – Możliwość instalacji min. dwóch wersji oprogramowania – firmware. – Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash.	

	– Możliwość monitorowania zajętości CPU. – Możliwość monitorowania zajętości pamięci. – Wsparcie mirroringu ruchu: lokalny mirroring na przełączniku, zdalny mirroring, zdalny mirroring do wskazanego adresu IP poprzez tunel – np. GRE, możliwość mirroringu ruchu wybranego za pomocą listy kontroli dostępu ACL. – Wsparcie diagnostyki okablowania – wykrywanie przerwy, zwarcia oraz odległości do awarii.	
Funkcje L2 przełącznika	Tablica MAC adresów min. 32 tys.; obsługa sieci wirtualnych IEEE 802.1Q – min. 4 tys.; obsługa funkcjonalności Private VLAN – blokowanie ruchu pomiędzy klientami z możliwieniem łączności do wspólnych zasobów sieciowych; obsługa Q-in-Q IEEE 802.1ad; wsparcie dla ramek Jumbo Frames (min. 9216 bajtów); obsługa STP (Spanning Tree Protocol) IEEE 802.1D; obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w; obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s; obsługa PVST+ (Per-VLAN Spanning Tree Protocol); obsługa min. 64 instancji MSTP; obsługa Link Aggregation IEEE 802.3ad wraz z LACP: obsługa min. 128 grup łączy typu Link Aggregation, obsługa umożliwiająca zgrupowanie min. 8 portów; obsługa MLAG (Multi Chassis Link Aggregation); obsługa protokołu EAPS – RFC 3619; obsługa protokołu ERPS / G.8032; obsługa Quality of Service: rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p, rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym, obsługa kolejek Strict Priority, obsługa kolejek Weighted Round Robin, obsługa WRED (Weighted Random Early Detection); obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB; obsługa LLDP Media Endpoint Discovery (LLDP-MED); obsługa CDPv1 oraz CDPv2; przełącznik musi posiadać obsługę AVB (Audio Video Bridging); kontrola sztormów: możliwość ograniczenia liczby pakietów Multicast na porcie, możliwość ograniczenia liczby pakietów Broadcast na porcie, możliwość ograniczenia liczby pakietów Unknown Unicast na porcie; przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP; wsparcie DCB (Data Center Bridging): DCBX – Data Center Bridging eXchange, PFC – Priority-based Flow Control, ETS – Enhanced Transmission Selection.	
Funkcje L3 przełącznika IPv4	Obsługa min. 1500 interfejsów IP; wsparcie dla IP multinetting – wiele adresów przypisanych do jednej sieci VLAN; sprzętowa obsługa routingu IPv4; pojemność sprzętowej tabeli routingu min. 12 tys. wpisów; obsługa routingu statycznego IPv4; obsługa routingu dynamicznego IPv4: RIP v1/v2, OSPFv2 min. 4 aktywne interfejsy IP – możliwość rozszerzenia do pełnej funkcjonalności przez licencję, BGPv4 min. 2 sąsiadów – możliwość rozszerzenia do pełnej funkcjonalności przez licencję, ISIS – możliwość rozszerzenia przez licencję; obsługa redundancji routingu VRRP dla IPv4; Policy Based Routing dla IPv4; obsługa DHCP Relay; obsługa DHCP Relay z możliwością	

	wysłania zapytań jednocześnie do min. 4 serwerów; obsługa Opcji 82 dla DHCP.	
Funkcje L3 przełącznika IPv6	Sprzętowa obsługa routingu IPv6; pojemność tabeli routingu min. 6 tys. wpisów; obsługa routingu statycznego IPv6; obsługa routingu dynamicznego IPv6: RIPng, OSPFv3 min. 4 aktywne interfejsy IP – możliwość rozszerzenia do pełnej funkjconalności przez licencję, BGPv4 min. 2 sąsiadów – możliwość rozszerzenia do pełnej funkcjonalności przez licencję, ISIS – możliwość rozszerzenia przez licencję; obsługa redundancji routingu VRRP dla IPv6; Policy Based Routing dla IPv6; obsługa 6to4 (RFC 3056); opcja IPv6 Router Advertisement dla DNS – RFC 6106.	
Obsługa ruchu rozgłoszeniowego	Statyczne przyłączania portu do grupy multicast; filtrowanie IGMP; obsługa IGMP v1 – RFC 1112; obsługa IGMP v2 – RFC 2236; obsługa IGMP v3 – RFC 3376; obsługa IGMP v1/v2/v3 snooping; obsługa PIM-SM; obsługa PIM-DM – możliwość rozszerzenia przez licencję; obsługa PIM-SSM – możliwość rozszerzenia przez licencję; obsługa MLDv1 snooping; obsługa MLDv2 snooping; obsługa MVR (Multicast VLAN Registration).	
Funkcje bezpieczeństwa	Obsługa logowania do sieci Network Login: IEEE 802.1x based Network Login, MAC address based Network Login, Web based Network Login; obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants); obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation; przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x; przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication; automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink; automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging; automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA; automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA; przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów; obsługa Guest VLAN dla IEEE 802.1x; możliwość przekierowania klienta na Captive Portal podczas logowania do sieci; obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176; obsługa wymuszania ponownego periodycznego	

	uwierzytelnienie (Reauthentication); obsługa RADIUS Authentication (RFC 2865); obsługa RADIUS Accounting (RFC 2866); obsługa RADIUS Per-Command Authentication – uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS; obsługa RADIUS Authentication over TLS (RadSec); obsługa RADIUS Accounting over TLS (RadSec); obsługa TACACS+ (RFC 1492); bezpieczeństwo MAC adresów: ograniczenie liczby MAC adresów na porcie, zatrzaśnięcie MAC adresów na porcie, możliwość wpisania statycznych MAC adresów na port/vlan; możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning); dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4: – adres MAC źródłowy i docelowy plus maska, – adres IP źródłowy i docelowy plus maska dla IPv4, – adres IP źródłowy i docelowy plus maska dla IPv6, – protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd., – numery portów źródłowych i docelowych TCP, UDP, – zakresy portów źródłowych i docelowych TCP, UDP, – identyfikator sieci VLAN – VLAN ID, – Quality of Service IEEE 802.1p, – Quality of Service DiffServ/DSCP, – flagi TCP, – obsługa fragmentów; listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika; możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI; wsparcie 8 tys. wpisów ACL na wejściu (Ingress); wsparcie 1 tys. wpisów ACL na wyjściu (Egress); obsługa IP Security: Trused DHCP Server, DHCP Snooping and Guard, Gratuitous ARP Protection, DHCP Secured ARP/ARP Validation, IP Source Guard; ograniczenie przepustowości (rate limiting) na portach wyjściowych; ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL; obsługa wykrywania periodycznego zaniku linku (Port-Flap): możliwość zdefniowania liczby zaniku linku w czasie określonego czasu, możliwość automatycznej reakcji polegającej na wyłączeniu portu, możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas, możliwość raportowania zdarzenia poprzez Syslog, możliwość raportowania zdarzenia poprzez Trap SNMP; możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE – GCM-AES-128; możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE – GCM-AES-256; wydajność MACSec po rozbudowie przełącznika nie mniejsza niż: 25 Gb/s.	

Zarządzanie	Zarządzenia przez SNMP v1/v2/v3; obsługa SNMP Traps; obsługa synchronizacji czasu SNTP lub NTP; obsługa DNS klienta; zarządzanie przez przeglądarkę www – protokół http i https; możliwość zarządzania przez protokół XML; obsługa serwera SSH dla IPv4; obsługa serwera SSH dla IPv6; obsługa klienta SSH dla IPv4; obsługa klienta SSH dla IPv6; obsługa serwera Telnet dla IPv4; obsługa serwera Telnet dla IPv6; obsługa klienta Telnet dla IPv4; obsługa klienta Telnet dla IPv6; obsługa transferu plików: TFTP, SFTP, SCP; obsługa SYSLOG; obsługa Secure SYSLOG (TLS); obsługa SYSLOG – konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń; obsługa logowania komend CLI do logu systemowego; obsługa logowania komend do serwera SYSLOG; obsługa ping dla IPv4 i IPv6; obsługa traceroute dla IPv4 i IPv6; obsługa RMON min. 4 grupy: Status, History, Alarms, Events; obsługa RMON2.	
Inne	Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników; wbudowany DHCP Server; DHCP Server z możliwość definicji opcji (np. opcje 43, 60, 78 itp.); wbudowany DHCP Client; obsługa skryptów CLI; obsługa funkcji TCL/Tk w skryptach CLI; obsługa skryptów Python 3.x; możliwość uruchamiania skryptów: ręcznie z CLI przez administratora, o określonym czasie lub co wskazany czas, na podstawie zdarzeń z logu systemowego; możliwość edycji skryptów bezpośrednio na urządzeniu – system operacyjny musi zawierać edytor plików tekstowych; wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging.	
Zgodność z normami	EU RoHS – 2011/65/EU; EN/ETSI 300 019-2-1 v2.1.2 – Class 1.2 Storage; EN/ETSI 300 019-2-2 v2.1.2 – Class 2.3 Transportation; EN/ETSI 300 019-2-3 v2.1.2 – Class 3.1e Operational.	
Gwarancja	Dożywotnia gwarancja na sprzęt – min. 5 lat po zakończeniu produkcji; dożywotnia aktualizacja oprogramowania na przełączniku.	

System NAC:

Producent	
Nazwa	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Podstawowa funkcjonalność systemu NAC	– System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. – System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor). – System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z	

	jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. – System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. – System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. – System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. – System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. – Licencja ma być zwalniana po rozłączeniu urządzenia końcowego. – System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. – System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: VM – min. VMWare ESXi, co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x, maszyny fizyczne – serwery wspierane przez producenta. – System musi posiadać funkcjonalność serwerów: serwera RADIUS dla infrastruktury sieciowej, serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+, serwera SYSLOG, serwera TACACS+, serwera Monitoringu, serwera DHCP, serwera polityk uwierzytelniania i kontroli dostępu 802.1X, serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. – System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. – System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. – System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min	

	MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. – System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now. – Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. – System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. – System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. – System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. – System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie. – System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status). – System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania. – Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). – System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci. – System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. – System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.	

	– System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. – System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP. – Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, autoryzacji, statusu, opisu. – System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. – System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. – System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci. – System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. – System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+. – System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. – System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD). – System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google, LinkedIn. – System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS. – System musi posiadać funkcję personalizacji strony gościnnej. – Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon. – Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor. – Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS. – Captive Portal musi umożliwiać logowanie za pomocą kont	

	lokalnych oraz Microsoft Active Directory. – Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory. – Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu. – Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru. – Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). – Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP. – Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni. – Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. – System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. – System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego. – System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. – System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. – System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych. – System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. – System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc). – System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA. – System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni	

	sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej: czy system jest aktualny z możliwością automatycznego naprawienia niezgodności, czy włączony jest firewall, czy jest uruchomiony system antywirusowy i aktualna baza sygnatur, czy jest włączone szyfrowanie dysku systemowego, czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory, czy na dysku znajdują się pliki lub katalogi wskazane przez administratora, czy w systemie są uruchomione procesy wskazane przez administratora, czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności, czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: wartości klucza rejestru, typu wartości: Number, String, Version. – System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. – System musi współpracować z serwerem tokenów. – System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej: Microsoft Windows, Mac OS, iOS, Android. – System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). – System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.	
Mechanizmy uwierzytelniania	– System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. – System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: MAC, PAP/ASCII, CHAP, SNMP, 802.1X. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp. – System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. – System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. – System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). – System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: Tożsamość/Urządzenie końcowe, Grupa tożsamości/urządzeń końcowych, Parametry urządzeń	

	końcowych, min: system operacyjny, wersja, Atrybuty Active Directory, Jednostka organizacyjna tożsamości/urządzeń końcowych, Urządzenia sieciowe sieci przewodowej, bezprzewodowej, Grupy urządzeń sieciowych, Porty urządzeń sieciowych, Grupy portów urządzeń sieciowych, Jednostka organizacyjna portów, Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), Data, czas ważności polityki, Wewnętrzny Captive Portal, Metoda autoryzacji. – System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks. – System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC. – System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI. – System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. – System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. – System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV. – System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. – System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal. – System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. – System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. – System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. – System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.	

	– System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.	
Obsługa serwerów certyfikatów CA	– System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. – Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności: możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych; możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych; możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol); usługę OCSP (Online Certificate Status Protocol).	
Obsługa serwerów DHCP	– System musi posiadać funkcję zintegrowanego serwera DHCP. – System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. – System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP: uruchamianie usługi dla wybranych podsieci; przypisanie ustalonego adresu IP dla adresu MAC; przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci; możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC; możliwość określania braku dostępu dla wybranych adresów MAC; monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC; możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP; możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego; możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi; dokonywanie zmian bez konieczności wyłączania usług.	
Obsługa serwerów TACACS+	System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych: – System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. – System musi umożliwiać tworzenia haseł administratorom. – System musi umożliwiać tworzenie listy komend uprawnień dla administratorów. – System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. – System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. – System musi umożliwiać logowanie za pomocą	

	poświadczeń Microsoft Active Directory. – System musi wspierać logowanie administratorów za pomocą tokenów OTP. – System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.	
Raportowanie i monitoring	System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów: – Monitoring autoryzacji. – Monitoring dla zdarzeń systemowych. – Monitoring dla zdarzeń DHCP. – Monitoring dla tożsamości. – Monitoring dla urządzeń końcowych. – Monitoring dla urządzeń sieciowych. – Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. – Raport ze zdarzeń logowania z informacją o nadam adresie IP. – Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. – Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. – System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. – System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. – System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. – System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. – System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. – System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi. – Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. – Raport zdarzeń Microsoft Active Directory, minimum:	

	logowania, wylogowania z system w tym błędne logowania, logowania do sieci 802.1X.	
Alarmy	– System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: wiadomości e-mail, Syslog, notyfikacji systemowych. – Alarmy mogą być generowane w sytuacjach, min: ilości obsługiwanych transakcji RADIUS, opóźnienie obsługi transkacji RADIUS, statusu krytycznego modułów. – System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: badanie łączności IP za pomocą ping, traceroute; tcpdump protokołów RADIUS, TACACS+; wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty, wykonanie zdalnego polecenia na urządzeniu sieciowym.	
Wymagania dotyczące wdrożenia i harmonogram ramowy	– Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta. – Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA). – Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.). – Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list). – Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach. – Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy. – Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy. – Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6 h dziennie. – Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.	
Szkolenia/warsztaty	– Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC. – Warsztaty zostaną przeprowadzone dla 2 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC. – Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi	

	systemu NAC. – Warsztaty odbędą się na miejscu w siedzibie klienta. – Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej. – Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.	
Licencja wsparcia technicznego producenta oprogramowania	Wykonawca dostarczy wraz dożywotnią licencją systemu NAC 12 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum: – Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC. – Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia. – Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. – Dostęp do dokumentacji i instrukcji na stronie internetowej. – Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.	

....., dn. .....

.....

Podpis/-y osób uprawnionych do składania świadczeń woli w imieniu Wykonawcy oraz pieczątka imienna / pieczątki

Załącznik nr 3 do SWZ

(Niniejszy projekt umowy zawiera zapisy dla wszystkich części przedmiotu zamówienia, ale ostatecznie umowy zostaną sporządzone osobno dla każdej z dwóch części przedmiotu zamówienia. Zamawiający kolorem czerwonym oznaczył miejsca, w których treść umowy będzie różna zależnie od tego, jaką część zamówienia będzie obejmowała.)

UMOWA Nr ….. /2025

zawarta w dniu …… 2025 r. pomiędzy:
Gminą Sławno – Urząd Gminy Sławno z siedzibą przy ul. I Pułku Ułanów 11, 76-100 Sławno, NIP 4990523666, reprezentowaną przez Wójta Gminy Sławno – Krzysztofa Jędrzejczyka, (zwaną dalej „Zamawiającym”),
a
……
z siedzibą w ……., NIP ……..
reprezentowanym przez **……**
(zwanym dalej „Wykonawcą”),

w wyniku postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym na podstawie art. 275 ust. 1 została zawarta umowa o następującej treści:

§ 1

(Umowy sporządzone zostaną osobno dla każdej z dwóch części przedmiotu zamówienia, a ostateczna treść § 1 umowy dotyczyła będzie wyłącznie części, na którą złożona została oferta Wykonawcy.)

Część nr 1:
„1. Przedmiotem zamówienia jest dostawa serwerów, macierzy pamięci masowej, systemów operacyjnych wraz z usługami oraz zasilaczy awaryjnych.”

Część nr 2:
„1. Przedmiotem zamówienia jest rozszerzenie obecnego UTM o funkcję HA wraz z wdrożeniem, dostawa systemu bezpiecznego zdalnego dostępu wraz z wdrożeniem, systemu do kontroli poczty elektronicznej wraz z wdrożeniem. Dostawa przełączników sieciowych. Dostawa, wdrożenie i konfiguracja NAC.”

2. Niniejsze zamówienie współfinansowane jest w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.

§ 2

1. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.
2. Wymagania ogólne:
   6) O ile inaczej nie zaznaczono, wszelkie zapisy SWZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
   7) Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2024 r., wolny od

jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie „fabrycznie nowy” należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez „wadę fizyczną” należy rozumieć również jakąkolwiek niezgodność ze opisem przedmiotu zamówienia.

8) Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania software’owe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu.
9) Dokumenty gwarancyjne wystawiane i przekazywane przez Wykonawcę powinny być zgodne z zapisami SWZ.
10) Oprogramowanie pochodzić będzie z legalnego, tj. akceptowanego przez producenta Oprogramowania kanału dystrybucji oraz zostanie udostępnione Zamawiającemu do korzystania na warunkach stosowanych lub akceptowanych przez takiego producenta.

3. Szczegółowy opis dostarczanego sprzętu określony został w załączniku nr …….. (2a lub 2b) do SWZ stanowiącym załącznik do oferty Wykonawcy.
4. Kryteria równoważności:
   1) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
   2) W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm polskich lub europejskich, ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 5 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
   3) Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SWZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

§ 3

Wykonawca dostarczy przedmiot zamówienia w terminie 90 dni od dnia podpisania umowy.

§ 4

(Umowy sporządzone zostaną osobno dla każdej z dwóch części przedmiotu zamówienia, a ostateczna treść § 4 umowy dotyczyła będzie wyłącznie części, na którą złożona została oferta Wykonawcy.)

Część nr 1:

„1. Za wykonanie przedmiotu umowy określonego w § 1 i 2 wynagrodzenie ustalone na podstawie oferty wynosi:

1) Wartość netto: …….. zł,
2) VAT – …….. %: ……..… zł,
3) **Wartość brutto: …….. zł,**
4) Słownie: …….

2. Wynagrodzenie określone w ust. 1 niniejszego paragrafu, obejmuje całość kosztów związanych z realizacją przedmiotu umowy i nie podlega zmianie w trakcie jej wykonywania.
3. Wykonawcy poza kwotą wynagrodzenia, określoną w ust. 1 niniejszego paragrafu, nie przysługują żadne roszczenia majątkowe wobec Zamawiającego z tytułu wykonania przedmiotu umowy.
4. Wynagrodzenie będzie wypłacone po wykonaniu całości przedmiotu zamówienia.
5. Termin płatności wynosi …….. dni od dnia otrzymaniu prawidłowo wystawionych faktur.
6. Forma płatności: przelew na konto bankowe Wykonawcy wskazane na fakturze. Rachunek bankowy Wykonawcy musi być zgodny z numerem rachunku ujawnionym w wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, prowadzonym przez Szefa Krajowej Administracji Skarbowej, zwanym dalej „wykazem”. Gdy w wykazie ujawniony będzie inny rachunek bankowy, płatność wynagrodzenia dokonana zostanie na rachunek bankowy ujawniony w wykazie. W przypadku, gdy Wykonawca nie figuruje w wykazie zobowiązany jest ujawnić swój numer rachunku bankowego w wykazie. Zamawiający wstrzyma do czasu ustania przyczyny płatność faktury w przypadku niewywiązania się Wykonawcy z zobowiązania ujawnienia rachunku bankowego w wykazie. Wstrzymanie wypłaty wynagrodzenia nie rodzi w tych przypadkach po stronie Zamawiającego opóźnienia i Wykonawcy nie przysługują odsetki z tego tytułu.
7. Podstawą zapłaty za realizację przedmiotu umowy będzie faktura wystawiona przez Wykonawcę na następujące dane:
   NABYWCA:
   Gmina Sławno, ul. I Pułku Ułanów 11, 76-100 Sławno,
   NIP: 499-052-36-66,
   PŁATNIK – ODBIORCA:
   Urząd Gminy Sławno, ul. I Pułku Ułanów 11, 76-100 Sławno.
8. W przypadku nieterminowej płatności Wykonawcy za opóźnienie przysługują odsetki ustawowe.”

Część nr 2:

„1. Za wykonanie przedmiotu umowy określonego w § 1 i 2 wynagrodzenie ustalone na podstawie oferty wynosi:

1) Wartość netto: …….. zł,
2) VAT – …….. %: ……..… zł,
3) **Wartość brutto: …….. zł,**
4) Słownie: …….

2. Wynagrodzenie określone w ust. 1 niniejszego paragrafu, obejmuje całość kosztów związanych z realizacją przedmiotu umowy i nie podlega zmianie w trakcie jej wykonywania.

3. Wykonawcy poza kwotą wynagrodzenia, określoną w ust. 1 niniejszego paragrafu, nie przysługują żadne roszczenia majątkowe wobec Zamawiającego z tytułu wykonania przedmiotu umowy.
4. Wynagrodzenie będzie wypłacone na podstawie jednej faktury częściowej, której wartość nie może przekroczyć 60% wynagrodzenia brutto Wykonawcy oraz faktury końcowej po podpisaniu protokołu końcowego.
5. Płatność częściowa nastąpi w oparciu o fakturę częściową wystawioną po podpisaniu bez uwag protokołu zdawczo – odbiorczego potwierdzającego dostarczenie sprzętu.
6. Ostateczne rozliczenie za wykonanie przedmiotu umowy nastąpi w oparciu o fakturę końcową wystawioną po podpisaniu protokołu końcowego bez uwag.
7. Termin płatności wynosi …….. dni od dnia otrzymaniu prawidłowo wystawionych faktur.
8. Forma płatności: przelew na konto bankowe Wykonawcy wskazane na fakturach. Rachunek bankowy Wykonawcy musi być zgodny z numerem rachunku ujawnionym w wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, prowadzonym przez Szefa Krajowej Administracji Skarbowej, zwanym dalej „wykazem”. Gdy w wykazie ujawniony będzie inny rachunek bankowy, płatność wynagrodzenia dokonana zostanie na rachunek bankowy ujawniony w wykazie. W przypadku, gdy Wykonawca nie figuruje w wykazie zobowiązany jest ujawnić swój numer rachunku bankowego w wykazie. Zamawiający wstrzyma do czasu ustania przyczyny płatność faktury w przypadku niewywiązania się Wykonawcy z zobowiązania ujawnienia rachunku bankowego w wykazie. Wstrzymanie wypłaty wynagrodzenia nie rodzi w tych przypadkach po stronie Zamawiającego opóźnienia i Wykonawcy nie przysługują odsetki z tego tytułu.
9. Podstawą zapłaty za realizację przedmiotu umowy będą faktury wystawione przez Wykonawcę na następujące dane:
   NABYWCA:
   Gmina Sławno, ul. I Pułku Ułanów 11, 76-100 Sławno,
   NIP: 499-052-36-66,
   PŁATNIK – ODBIORCA:
   Urząd Gminy Sławno, ul. I Pułku Ułanów 11, 76-100 Sławno.
10. W przypadku nieterminowej płatności Wykonawcy za opóźnienie przysługują odsetki ustawowe.”

§ 5

1. Wykonawca zobowiązany jest do wykonania przedmiotu umowy zgodnie z postanowieniami SWZ, przepisami prawa i obowiązującymi w tym zakresie normami technicznymi.
2. Wykonawca, który powołuje się na rozwiązania równoważne opisane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy, spełniają wymagania określone przez Zamawiającego. Obowiązek Wykonawcy wykazania równoważności produktu jest obowiązkiem wynikającym z ustawy, który może być spełniony w jakikolwiek sposób pozwalający Zamawiającemu jednoznacznie stwierdzić zgodność oferowanych w ofercie produktów z wymaganiami określonymi w SWZ.

§ 6

1. Wykonawca poza gwarancjami producentów sprzętu udzieli własnej gwarancji na prace wdrożeniowe na okres 12 miesięcy od dnia odebrania przez Zamawiającego przedmiotu umowy (bez uwag).
2. Jeżeli w toku czynności odbioru zostaną stwierdzone wady Zamawiający ma prawo do:

1) jeżeli wady nadają się do usunięcia – odmowy odbioru przedmiotu umowy do czasu usunięcia wad, wyznaczając termin na ich usunięcie,
2) jeżeli wady nie nadają się do usunięcia, to:
   a) gdy wady umożliwiają prawidłowe użytkowanie przedmiotu dostawy zgodnie z przeznaczeniem – Zamawiający może żądać obniżenia odpowiednio wynagrodzenia Wykonawcy,
   b) gdy wady uniemożliwiają prawidłowe użytkowanie przedmiotu dostawy zgodnie z przeznaczeniem – Zamawiający może odstąpić od umowy lub żądać dostawy nowego przedmiotu umowy.

3. Wykonawca jest zobowiązany do pisemnego zawiadomienia Zamawiającego o usunięciu wad oraz do żądania wyznaczenia terminu do odbioru zakwestionowanego przedmiotu dostawy.
4. W przypadku opóźnienia w terminie usunięcia wad stwierdzonych podczas odbioru Zamawiający naliczy Wykonawcy kary umowne, o których mowa w § 7 ust. 1 pkt. 2 umowy.
5. Jeżeli w ramach rękojmi za wady lub gwarancji jakości, Wykonawca usunął wadę istotną, termin rękojmi lub gwarancji biegnie na nowo od chwili usunięcia wady. W pozostałych przypadkach termin rękojmi lub gwarancji ulega przedłużeniu o czas, w którym wada była usuwana. Zarzut z tytułu rękojmi za wady oraz gwarancji jakości Zamawiający może podnieść po upływie terminów określonych w niniejszym paragrafie, jeżeli przed ich upływem zawiadomił Wykonawcę o wadzie.

§ 7

1. Strony ustalają, że Wykonawca zapłaci Zamawiającemu kary umowne z następujących tytułów:
   1) za zwłokę w wydaniu przedmiotu umowy w wysokości 0,2% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3 za każdy dzień zwłoki;
   2) za zwłokę w usunięciu braków, wad lub usterek stwierdzonych przy odbiorze lub w okresie rękojmi za wady w wysokości 0,2% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3 za każdy dzień zwłoki liczony od dnia wyznaczonego na usunięcie wad;
   3) za odstąpienie przez Zamawiającego od umowy z powodu okoliczności, za które odpowiada Wykonawca w wysokości 10% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3;
   4) za odstąpienie przez Wykonawcę od umowy z powodu okoliczności, za które odpowiada on sam w wysokości 10% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3.
2. Łączna wysokość kar umownych naliczonych Wykonawcy przez Zamawiającego nie może przekroczyć 20 % kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3.
3. Zamawiający zastrzega sobie, a Wykonawca wyraża zgodę, na potrącenie należności wynikających z kar umownych z przysługującego Wykonawcy wynagrodzenia za wykonanie przedmiotu umowy.
4. Postanowienia ust. 1 nie wyłączają prawa Zamawiającego do dochodzenia od Wykonawcy odszkodowania uzupełniającego na zasadach ogólnych, jeżeli wartość powstałej szkody przekroczy wysokość kar umownych.
5. W razie zaistnienia istotnej zamiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia

wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.

§ 8

1. Zamawiający przewiduje możliwość dokonania zmiany postanowień umowy na podstawie art. 455 ustawy Prawo zamówień publicznych, które zostaną wyrażone w formie pisemnego aneksu pod rygorem nieważności i mogą nastąpić wyłącznie w następujących sytuacjach:
   2) zmiany terminu wykonania umowy, w przypadku:
      d) wystąpienia okoliczności, których nie można było przewidzieć w chwili zawarcia umowy,
      e) wstrzymanie realizacji przedmiotu umowy przez Zamawiającego nie wynikające z przyczyn leżących po stronie Wykonawcy,
      f) wyrażenia zgody przez Zamawiającego na skrócenie terminu realizacji,
   3) w zakresie zmiany wynagrodzenia, zwłaszcza w sytuacji zmiany stawki obowiązującego podatku od towarów i usług (VAT).
2. Warunkiem dokonania zmian, o których mowa w ust. 1, jest złożenie wniosku przez stronę inicjującą zmianę zawierającego:
   5) opis propozycji zmiany,
   6) uzasadnienie zmiany,
   7) obliczenie kosztów zmiany zgodnie z zasadami określonymi w umowie, jeżeli zmiana będzie miała wpływ na wynagrodzenie Wykonawcy,
   8) opis wpływu zmiany na harmonogram realizacji i fakturowania oraz termin wykonania umowy.
3. Wykonawca nie będzie uprawniony do żądania przedłużenia terminu wykonania umowy i zwiększenia wynagrodzenia, jeżeli zmiana jest wymuszona uchybieniem czy naruszeniem umowy przez Wykonawcę – w takim przypadku koszty dodatkowe związane takimi zmianami ponosi Wykonawca.
4. Powyższe zmiany nie mogą być niekorzystne dla Zamawiającego.
5. Poza przypadkami opisanymi w niniejszym paragrafie, zmiana umowy może nastąpić w przypadkach przewidzianych w art. 455 ust. 1 pkt. 2 – 4 i ust. 2 ustawy Prawo zamówień publicznych.

§ 9

1. W kwestiach nieuregulowanych niniejszą umową mają zastosowanie postanowienia ustawy Prawo zamówień publicznych i Kodeksu Cywilnego.
2. Ewentualne spory wynikłe w związku z realizacją umowy będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
3. Niniejszą umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego oraz jeden egzemplarz dla Wykonawcy.
4. Integralnymi częściami niniejszej umowy są:
   1) Oferta Wykonawcy.
   2) SWZ.
   3) Gwarancja.

WYKONAWCA: ***ZAMAWIAJĄCY:***

Załącznik nr 3 do umowy

GWARANCJA

1. Wykonawca..... zapewnia, że przedmiot umowy polegający na **„Dostawa urządzeń komputerowych w ramach realizacji projektu – Cyberbezpieczna Gmina Sławno”** został wykonany należycie.
2. Wykonawca gwarantuje dobrą jakość wykonanego przedmiotu powyższej umowy.
3. W razie stwierdzenia w okresie udzielonej gwarancji za wady, która wynosi 12 miesięcy od dnia odbioru (bez uwag i zastrzeżeń) przedmiotu umowy od Wykonawcy, wad i usterek w wykonanym przedmiocie umowy, Wykonawca zobowiązuje się je usunąć na swój koszt niezwłocznie po wezwaniu do ich usunięcia.
4. Ustalenie wad i usterek nastąpi protokolarnie z udziałem obu stron umowy.
5. Protokół, określający stwierdzone wady i usterki oraz sposób i termin ich usunięcia, zostanie spisany przez Zamawiającego.
6. Sporządzenie protokołu bez udziału zawiadomionego Wykonawcy ma taki sam walor jak protokół sporządzony z udziałem Wykonawcy.
7. Protokół stanowi wezwanie Wykonawcy do usunięcia wad i usterek w określonym w tym protokole terminie.
8. Jeżeli Wykonawca nie usunie wad i usterek w terminie określonym w protokole Zamawiającemu przysługuje prawo wykonania zastępczego na koszt i ryzyko Wykonawcy.

....., dn. .....

.....
Podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy oraz pieczątka / pieczątki

Załącznik nr 4 do SWZ

Nazwa wykonawcy .....

Adres wykonawcy .....

O Ś W I A D C Z E N I E

Na potrzeby postępowania o udzielenie zamówienia publicznego, pn. **„Dostawa urządzeń komputerowych w ramach realizacji projektu – Cyberbezpieczna Gmina Sławno”** prowadzonego przez Gminę Sławno oświadczam, co następuje:

1. nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust 1 ustawy Pzp;

2. nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 ustawy Pzp;

3. nie podlegam wykluczeniu z postępowania 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. z 2022, poz. 835 z późn. zm.);

4. *zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……..... ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 i 6 lub art. 109 ust. 1 pkt. 2-10 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:
   …….
   ……..…...
   ……..…

5. *następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:
   …….
   ……..…...
   ……..…
   nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia;

6. *następujący/e podmiot/y, będący/e podwykonawcą/ami:
   …….
   ……..…...
   ……..…
   nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia;

7. spełniam warunki udziału w postępowaniu określone przez zamawiającego w specyfikacji warunków zamówienia.

8. *w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w specyfikacji warunków zamówienia, polegam na zasobach następującego/ych podmiotu/ów:
   ……
   ……..…...
   ……..…
   w następującym zakresie:
   ……
   ……..…...
   ……..…

9. wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

10. zapoznaliśmy się z warunkami realizacji zamówienia publicznego oraz przyjmujemy je do realizacji bez zastrzeżeń.

11. zapoznaliśmy się ze specyfikacją warunków zamówienia, nie wnosimy do niej uwag ani zastrzeżeń

12. zapoznaliśmy się z formularzem projektu umowy (**Załącznik nr 3 do SWZ**) i nie wnosimy do niego zastrzeżeń.

13. zdobyliśmy wszelkie możliwe informacje w celu należytego przygotowania oferty, w tym określenia ceny naszej oferty.

14. udzielimy wszelkich możliwych wyjaśnień dotyczących złożonej przez nas oferty.

.....
Podpis wykonawcy

Miejscowość i data: .....

**niepotrzebne skreślić*

Załącznik nr 5 do SWZ

Oświadczenia wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 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. U. UE L z 2016 r. Nr 119 poz. 1 i z 2018 r. Nr 127 poz. 2)wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

.....
Podpis wykonawcy

Miejscowość i data: .....