Zamawiający:
Gmina Ładzice, ul. Wyzwolenia 36, 97-561 Ładzice

Załącznik nr 1

do Zapytania ofertowego nr ZPP.271.1.27.2025

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: Świadczenie usług szkoleniowych, aktualizacja dokumentacji SZBI – w tym opracowanie polityki zapewnienia ciągłości działania, audyt wdrożonego systemu SZBI, zgodności z KRI uKSC oraz zakup i wdrożenie Systemu klasy NAC zapewniającego kontrolę dostępu do sieci komputerowej urzędu w ramach projektu grantowego „Cyberbezpieczny samorząd" Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0630/ FERC.02.02-CS.01-001/23/2024, 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, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)

I. USŁUGI SZKOLENIOWE

1. Szkolenia stacjonarne z zakresu cyberbezpieczeństwa

1. Szkolenia z zakresu cyberbezpieczeństwa zostaną przeprowadzone w 2 grupach po 13 osób.
2. Szkolenie dla jednej grupy szkoleniowej powinno trwać minimum 3 godziny.
3. Wszystkie szkolenia muszą być prowadzone w siedzibie Zamawiającego w języku polskim na podstawie zaakceptowanego przez Zamawiającego harmonogramu i planu szkolenia, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 3 dni przed rozpoczęciem cyklu szkoleń.
4. Wykonawca wystawi dla każdego uczestnika szkolenia zaświadczenie o ukończeniu szkolenia.
5. Zamawiający wymaga prowadzenie dokumentacji szkoleń, na którą składają się: lista obecności uczestników szkolenia (odrębna dla każdej grupy szkoleniowej) oraz lista odbioru zaświadczeń po ukończeniu szkolenia.
6. Szkolenia dla pracowników muszą obejmować minimum następujące zagadnienia:
   1) podstawowe wiadomości w zakresie bezpieczeństwa informacji, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI, uKSC oraz RODO,

2) zasady bezpiecznego korzystania z Internetu (cyberhigiena),
3) hacking, malware jako zagrożenie,
4) ransomware jako poważne zagrożenie dla JST,
5) ataki związane z użyciem urządzeń wymiennych,
6) inżynieria socjotechniczna (phishing, wyłudzenia z uwzględnieniem oszustwa typu BEC - Business Email Compromise),
7) zabezpieczanie urządzeń mobilnych i ochrona danych osobowych,
8) bezpieczne hasła i uwierzytelnianie dwuskładnikowe,
9) identyfikacja podejrzanych wiadomości e-mail, rozpoznawanie zagrożeń,
10) zasady postępowania w przypadku, gdy doszło do wycieku danych,
11) procedury zgłaszania incydentów.

7. Zamawiający wymaga, aby szkolenia były przeprowadzone przez podmiot posiadający min. 3-letnie doświadczenie w prowadzeniu szkoleń oraz w tym okresie przeprowadził co najmniej 5 szkoleń dla pracowników jednostek samorządu terytorialnego popartych referencjami. W celu uzyskania odpowiedniego efektu szkolenia dodatkowo punktowane będzie posiadanie przez trenera (osobę prowadząca szkolenia) przygotowania pedagogicznego. **– Czy to będzie dodatkowe kryterium przy ocenie ofert np. przygotowanie pedagogiczne 20% cena 80%?**

2. **Dostęp do platformy umożliwiającej przeprowadzenie kampanii phishingowych i edukacyjnych**

1. Zamawiający wymaga prowadzenia kampanii phishingowej i edukacyjnej z wykorzystaniem dedykowanej platformy, dostępnej w wersji chmurowej (SaaS).

2. Platforma szkoleniowa musi umożliwić jednoczesne korzystanie 26 osób przez okres minimum 4 miesięcy.

3. Wymagania ogólne dla platformy:
   1) Rozwiązanie musi posiadać swoje centrum danych na terenie Unii Europejskiej.
   2) Konsola centralna platformy musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS.
   3) Administrator w konsoli centralnej musi posiadać możliwość dodania dodatkowych użytkowników zarządzających.
   4) Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.

4. Prowadzenie kampanii phishingowych i edukacyjnych:
   1. rozwiązanie musi posiadać możliwość utworzenia kampanii phishingowej i edukacyjnej;
   2. możliwość tworzenia własnych profili phishingowych lub importu predefiniowanych na platformie;
   3. profile kampanii phishingowych dostępne na platformie muszą być minimum w wersji polskiej i angielskiej;

4. profil kampanii phishingowej musi zawierać szablon wiadomości e-mail lub wiadomości e-mail i strony internetowej;
5. rozwiązanie musi posiadać możliwość przypisania do profilu kampanii phishingowej kategorii domen, z których wysyłane będą wiadomości;
6. kampanie phishingowe muszą posiadać możliwość wyboru czasu rozpoczęcia kampanii oraz sposobu wysyłania wiadomości (wysyłane jednorazowo do wszystkich odbiorców, wysyłane w grupach, wysyłane losowo w określonym zakresie czasu);
7. platforma musi posiadać co najmniej 5 predefiniowanych szablonów kampanii w minimum języku polskim:
   a) wiadomości phishingowe - oszustwo związane z kontem e-mail,
   b) wiadomości phishingowe i strony internetowe - oszustwa związane z kontami e-mail,
   c) wiadomości phishingowe i strony internetowe - oszustwa związane z kartami kredytowymi,
   d) pobieranie plików - Office 365,
   e) phishing - Office 365;
8. możliwość przypisania do kampanii phishingowej, kampanii edukacyjnej przeprowadzanej poprzez wysłanie wiadomości e-mail i/lub strony internetowej;
9. możliwość utworzenia własnych profili edukacyjnych lub importu predefiniowanych przez producenta;
10. profile kampanii edukacyjnych utworzone przez producenta muszą być dostępne minimum w języku polskim i angielskim;
11. rozwiązanie musi posiadać możliwość wyboru treści wiadomości edukacyjnej w zależności od podjętej przez odbiorcę czynności: otwarcia wiadomości, odpowiedzi na wiadomość, kliknięcia w link oraz wypełnienia formularza na stronie phishingowej;
12. rozwiązanie musi posiadać możliwość stworzenia oraz wyboru treści prezentacji edukacyjnej w formie strony internetowej na której można zamieszczać treści edukacyjne w postaci tekstu, grafiki oraz wideo;
13. rozwiązanie musi posiadać możliwość stworzenia oraz wyboru testu sprawdzającego wiedzę w formie strony internetowej na której można zamieszczać pytania i odpowiedzi w formie jednokrotnego i wielokrotnego wyboru;
14. rozwiązanie musi posiadać możliwość anonimizacji danych odbiorców i podjętych przez nich czynności.

5. Raporty:
   1. Możliwość tworzenia raportów z oceny phishingu e-mail;
   2. Możliwość tworzenia raportu zgodności co najmniej z:
      a) przepisami o ochronie danych osobowych,
      b) wymogami w zakresie bezpieczeństwa informacji wg ISO 27001 lub równoważnej.
   3. Możliwość dostarczania nowych niestandardowych raportów zgodności;
   4. Możliwość tworzenia raportu trendów z historią podatności;
   5. Możliwość selektywnego raportowania podatności i wykluczenia (uwzględnione systemy operacyjne, filtry zasobów, filtry podatności);

6. Możliwość tworzenia "raportów skróconych" tygodniowych i miesięcznych, wysyłanych w sposób podsumowujący poprzez e-mail.

3. **Szkolenia e-learningowe**

1. Wymagana przez Zamawiającego podstawowa funkcjonalność systemu:

a) Oprogramowanie utrzymywane globalnie (model SAAS); możliwość korzystania z systemu bez dodatkowych aplikacji dedykowanych.

b) Możliwość logowania MFA z wykorzystaniem tokenów autoryzacyjnych Google/Microsoft Authenticator.

c) Dedykowane szkolenia obejmujące m.in. następujące zagadnienia:

- skuteczne metody ochrony przed phishingiem,
- bezpieczeństwo w usługach chmurowych,
- bezpieczeństwo w stosowaniu narzędzi opartych na sztucznej inteligencji,
- zagrożenia cyberbezpieczeństwa na przykładzie oprogramowania wymuszającego okup,
- bezpieczeństwo formularzy i socjotechnika,
- przykłady ataków,
- wytyczne dla podejścia „zero zaufania".

d) Funkcjonalność automatycznej analizy udzielanych odpowiedzi w ankietach.

e) Funkcjonalność automatycznej analizy realizowanych ścieżek szkoleniowych, w tym udzielanych odpowiedzi w czasie testów, celem opracowania raportu wskazującego najbardziej problematyczne obszary.

f) Ułatwienia dla osób słabowidzących, w tym powiększenie, zmiana kolorystyki.

g) Ułatwienia dla osób słabosłyszących, w tym transkrypcja audio.

h) Możliwość dodawania własnych szkoleń.

i) Możliwość dodawania własnych egzaminów ze skonfigurowaną punktacją np. pytania wielokrotnego wyboru z punktami ujemnymi.

j) Możliwość konfiguracji procesów onboardingowych z wymaganymi szkoleniami i egzaminami, tak by pracownik mógł odbyć szkolenie, zapoznać się z dokumentem, złożyć e-podpis, zdać egzamin, otrzymać certyfikat i upoważnienie do przetwarzania (automatycznie).

k) Możliwość określenia limitu czasu na cały egzamin oraz na poszczególne pytania w trakcie egzaminu.

l) Możliwość określenia wymaganych kursów oraz egzaminów, by umożliwić automatyczny dostęp do kolejnych np. na wyższym poziomie po ukończeniu wskazanych.

m) Możliwość dodawania/modyfikacji certyfikatów.

n) Kreator slajdów z prekonfigurowanymi slajdami szkoleniowymi.

o) Opisana funkcjonalność powinna być dostępna w bazowej wersji produktu z zagwarantowanymi aktualizacjami minimum 6 miesięcy przed ogłoszeniem postępowania, a nie opracowana po zakupie.

p) Zarządzanie uprawnieniami RBAC, w tym możliwość tworzenia grup lokalnych, definicja uprawnień dla właścicieli grupy. Możliwość definiowania dziedziczenia uprawnień.

q) Możliwość zmiany nazwy dla elementów menu wg wymagań Zamawiającego.

r) Możliwość realizacji szkoleń w symulowanym środowisku ataki phishingowe z monitorowaniem postępów - w ramach oferowanego systemu.

s) Oprogramowanie musi być dostępne z powszechnie stosowanych przeglądarek internetowych oraz z możliwością dostępu do wszystkich funkcjonalności na smartfonach i tabletach z Android/iOS/Windows.

t) Zamawiający oczekuje dostępów by zalogować się do systemu bez konieczności instalowania jakichkolwiek dodatkowych komponentów oprócz przeglądarki internetowej w aktualnej stabilnej wersji.

u) W ramach dostawy zostanie zapewniony dostęp do Systemu dla co najmniej 26 nazwanych użytkowników Zamawiającego przez okres 1 miesiąc w 2025 roku i 1 miesiąc w 1-szym kwartale 2026 roku.

2. Dostawa, gwarancja i usługa wdrożeniowa:

a) Zamawiający wymaga zapewnienia aktualizacji Systemu (asysta techniczna) oraz nieprzerwanego działania Systemu (SLA) przez cały okres dostępu do Systemu.

b) Ciągłość działania usługi musi być zapewniona bez konieczności zapewnienia hostingu przez Zamawiającego (System utrzymywany w formule SaaS).

c) Wykonawca lub producent Systemu zapewni wsparcie techniczne w godzinach pracy Zamawiającego.

d) Wykonawca lub producent Systemu zapewni SLA w formie czasu reakcji na zgłoszenia o problemach do 4 godzin oraz czasu naprawy w przypadku awarii Systemu, tj. niezgodności ze specyfikacją określoną w niniejszym opisie przedmiotu zamówienia do 5 dni roboczych.

e) Wdrożenie/udostępnienie Systemu zgodnie z wymaganiami Zamawiającego nastąpi w terminie do 30 dni od podpisania umowy.

f) Zamawiający oczekuje zapewnienia dokumentacji w formie elektronicznej z samouczkami w języku polskim

Zamawiający:

Gmina Ładzice, ul. Wyzwolenia 36, 97-561 Ładzice

II. AKTUALIZACJA DOKUMENTACJI SZBI ORAZ AUDYT WDROŻONEGO SZBI

1. Przedmiotem zamówienia jest usługa polegająca na aktualizacji w Urzędzie Gminy Ładzice dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI).

1.1. Celem aktualizacji dokumentacji SZBI jest zapewnienie wysokiego poziomu bezpieczeństwa informacji w urzędzie gminy oraz spełnienie wymagań:

a) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC),
b) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI),
c) dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz aktów wykonawczych wydanych do niej.

1.2. Zakres prac obejmuje:

a) Audyt wstępny SZBI polegający m.in. na sprawdzeniu i zrozumieniu środowiska Urzędu Gminy, obejmującego aktualną strukturę organizacyjną, system zarządzania realizowanych procesów oraz wymagania prawne funkcjonujące w urzędzie, inwentaryzację i analizę aktywów - zasobów informacyjnych oraz środków służących do gromadzenia i przetwarzania informacji, ocenę zgodności z KRI oraz KSC. Wyniki audytu będą podstawą do dalszych prac.
b) Aktualizację posiadanej dokumentacji SZBI, która obejmuje procesy, procedury, dokumenty, analizy ryzyka w bezpieczeństwie informacji oraz ciągłości działania i będzie przeprowadzona na podstawie wyników z audytu wstępnego SZBI. Wykonawca przeprowadzi przy udziale przedstawicieli Zamawiającego analizę ryzyka, w tym opracuje i wdroży metodykę zarządzania ryzykiem oraz wskaże obszary wymagające dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagane do wdrożenia zabezpieczenia. Wynikiem wdrożenia ma być zwiększenie cyberbezpieczeństwa, wprowadzenie i udokumentowanie SZBI, które pozwolą zapewnić zgodność podczas audytu końcowego. Opracowane polityki, procedury itd. muszą realnie odnosić się do procesów funkcjonujących w UG. Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem zrozumiałym dla osób nieposiadających wysokiego przygotowania z zakresu bezpieczeństwa informacji. Jednocześnie Zamawiający zastrzega, że wszelkie błędy w przygotowanej dokumentacji świadczące o tym, że dokumentacja została przeniesiona z innej

organizacji będą podstawą do odrzucenia dokumentów do poprawy, bez ich dalszej analizy ze strony Zamawiającego.

2. Audyt wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji

2.1. Przedmiotem zamówienia jest usługa przeprowadzenia audytu wdrożonego w Urzędzie Gminy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz zgodności z wymaganiami:

a) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC),
b) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI),
c) dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz aktów wykonawczych wydanych do niej.

2.2. Po przeprowadzeniu audytu wdrożonego u Zamawiającego SZBI, w tym uwzględnieniu zagadnień określonych w Załączniku Nr 6 do Regulaminu konkursu grantowego „Cyberbezpieczny Samorząd" Ankieta Dojrzałości Cyberbezpieczeństwa, Wykonawca opracuje raport z audytu.

2.3. Raport z audytu wdrożonego SZBI ma zawierać porównanie audytu wstępnego wykonanego przed opracowaniem i wdrożeniem SZBI. Raport z audytu powinien być podpisany przez audytora opracowującego audyt systemu (podpis kwalifikowany).

2.4. Zamawiający wymaga, aby Wykonawca dysponował:

a) co najmniej dwoma audytorami wiodącymi systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 posiadającymi aktualne certyfikaty potwierdzające posiadane uprawnienia wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób, oraz

b) co najmniej jednym audytorem wiodącym systemu zarządzania ciągłością działania według normy PN-EN ISO 22301 posiadającymi aktualne certyfikaty potwierdzające posiadane uprawnienia wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób.

2.5. Wykonawcy ubiegający się o realizację zamówienia powinni posiadać niezbędną wiedzę i doświadczenie oraz dysponować odpowiednimi zasobami osobowymi umożliwiającymi wykonanie przedmiotu zamówienia, a o udział w zamówieniu mogą ubiegać się Wykonawcy, którzy w okresie ostatnich 3 lat wykonali co najmniej: 5 usług przeprowadzenia audytów cyberbezpieczeństwa w podmiotach publicznych.

Zamawiający:

Gmina Ładzice, ul. Wyzwolenia 36, 97-561 Ładzice

III. SYSTEM KLASY NAC ZAPEWNIAJĄCY KONTROLĘ DOSTĘPU DO SIECI KOMPUTEROWEJ ZAMAWIAJĄCEGO

PODSTAWOWA FUNKCJONALNOŚĆ SYSTEMU NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).
3. 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.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 2500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. 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.
10. 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.
11. 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.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych,

poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.

13. 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.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. 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.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez e-mail.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. 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.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. login, hasło, imię, nazwisko, e-mail, status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. 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.
26. 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.

27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, autoryzacji, statusu, opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem SYSLOG informacji z serwerów autoryzacji, DHCP, VPN, OTP, TACACS+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. 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.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft

Active Directory.

45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. 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.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. 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.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM.
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS.
59. 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.

60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania informatyka urzędu co najmniej dla systemów: Microsoft Windows, Mac OS, iOS, Android.
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

MECHANIZMY UWIERZYTELNIANIA

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. 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.
3. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
4. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
5. 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).
6. 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.

7. 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.
8. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
9. 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.
10. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
11. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
12. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
14. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
15. 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.
16. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
17. 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.
18. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.

19. 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

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. 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

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. 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:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów

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

RAPORTOWANIE I MONITORING

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. 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 e-mail.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności VLANów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. 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.

16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów WiFi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum: logowania, wylogowania z system w tym błędne logowania, logowania do sieci 802.1X.

ALARMY

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
   - wiadomości e-mail,
   - Syslog,
   - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
   - Ilości obsługiwanych transakcji RADIUS,
   - Opóźnienie obsługi transkacji RADIUS,
   - Statusu krytycznego modułów.
3. 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:

1. Dostawa, instalacja, zalicencjonowanie Systemu NAC oraz konfiguracja zostanie wykonana w środowisku Zamawiającego.
2. Podstawowa konfiguracja Systemu NAC: integracja z domeną AD, konfiguracja urzędu certyfikacji.
3. Konfiguracja urządzenia firewall: dodatnie VLAN-u gościnnego, ustawienie polityk, etc.
4. Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
5. Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
6. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii; przeprowadzenie testów.

7. Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów; przeprowadzenie testów.
8. Przeprowadzenie szkolenia dla administratora sieci komputerowej Zamawiającego z konfiguracji i administrowania Systemem NAC.
9. Szczegółowy plan, zakres i termin szkolenia zostanie uzgodniony przez Wykonawcę z Zamawiającym.
10. Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 30 dni po zakończeniu wdrożenia.

LICENCJA WSPARCIA TECHNICZNEGO PRODUCENTA OPROGRAMOWANIA:
Wykonawca dostarczy wraz z dożywotnią licencją Systemu NAC – co najmniej do 30 czerwca 2026 **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.