Załącznik nr 1a

Część I

Rozszerzenie aktualnie posiadanego środowiska pracy w chmurze wraz z wdrożeniem oraz szkoleniem użytkowników

1. **Przedmiot zamówienia**
   1) Przedmiotem zamówienia jest rozszerzenie usługi pracy w chmurze.
   2) Dostawa 100 licencji w subskrypcji rocznej usługi przetwarzania danych w chmurze, dedykowanej celom biurowym wraz z dołączeniem ich do posiadanego przez Zamawiającego tenanta w usłudze Microsoft, jako rozszerzenie funkcjonalności wykorzystywanego środowiska MS365. Dostarczone licencje muszą być widoczne i zarządzalne z poziomu tenanta MS365
   3) Utworzenie kont użytkowniczych bazując na informacjach przekazanych przez Zamawiającego, przypisanie im dostarczonych licencji, uruchomienie skrzynek pocztowych dostępnych w ramach licencji oraz archiwizacja aktualnie użytkowanej przez pracowników Zamawiającego poczty elektronicznej
   4) Przeprowadzenie szkolenia powdrożeniowego dla użytkowników z obsługi rozwiązania.
   5) Obecnie zamawiający posiada aktywny tenant usługi chmurowej Microsoft 365 wraz z aktywnymi licencjami

2. Termin realizacji zamówienia

Termin realizacji zamówienia wynosi 60 dni od dnia podpisania umowy.

3. **Szczegółowe wymagania odnośnie dostawy licencji**

1) Ilekroć jest mowa o modelu licencyjnym należy przez to rozumieć pakiet biurowy w rozwiązaniu chmurowym.
2) Chmurowy pakiet biurowy, musi spełniać następujące wymagania:
   1. Wymagania odnośnie interfejsu użytkownika:
      a) Pełna polska wersja językowa interfejsu użytkownika.
      b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   2. Wymagane składowe chmurowego pakietu biurowego zwane usługami:
      a) Poczta e-mail i kalendarze - pojemność skrzynki 50GB, maksymalny rozmiar wiadomości 150MB,
      b) Przechowywanie i udostępnianie plików - każda licencja posiada przestrzeń w rozmiarze 1TB, dostępnej w postaci rozwiązania chmurowego w infrastrukturze Producenta
      c) Konferencje Online – do 300 osób,
      d) Wiadomości błyskawiczne i komunikator,
      e) Firmowa sieć społecznościowa,
      f) Witryny zespołów,
      g) Subskrypcja ma umożliwiać dostęp do internetowych wersji aplikacji pakietu chmurowego:
         I. klient poczty,
         II. edytor tekstu,
         III. arkusz kalkulacyjny,

IV. edytor prezentacji,
V. notes.
VI. Aplikacje muszą być dostępne z poziomu przeglądarki internetowej.

h) Usługa pocztowa,
i) Zarządzanie pracą,
j) Tworzenie biuletynów i prezentacji multimedialnych
k) Interfejs API dla usług wchodzących w skład oferowanego pakietu

3. Pakiet musi być kompatybilny z formatami dokumentów obsługiwanych i tworzonych u Zamawiającego za pomocą posiadanego oprogramowania pakietów biurowych – MS Office 2013-2019, MS 365.
4. Zamawiający wymaga dostępu do najnowszych wersji modelu subskrypcji przez cały okres jej ważności, tj. przez 12 miesięcy od dnia ich dostarczenia.
5. Dostarczone subskrypcje muszą być aktywne przez okres 12 miesięcy od daty przekazania ich Zamawiającemu, określonej umową (nie później niż 14 dni od jej podpisania).
6. Wymagana jest możliwość korzystania z pomocy w dowolnym momencie, dzięki całodobowej telefonicznej i internetowej pomocy technicznej od firmy dostawcy usługi.
7. Wykonawca musi zapewnić, że dostarczone subskrypcje są wolne od wad, dobrej jakości oraz ich parametry i cechy są zgodne z założeniami niniejszego dokumentu
8. Subskrypcje pakietu biurowego muszą zostać przypisane do aktualnie posiadanego przez Zamawiającego konta licencyjnego Microsoft 365 – centrum administracyjne na koncie Zamawiającego, nie później niż 14 dni pod podpisaniu umowy.

4. Wymagane prace wdrożeniowe

1) Walidacja oraz dostosowanie konfiguracji aktualnie posiadanej usługi zgodnie z najlepszymi praktykami, zapewniającymi prawidłową funkcjonalność rozwiązania celem zastąpienia aktualnej usługi pocztowej
2) Implementacja licencji w rozwiązaniu;
3) Zaimportowanie użytkowników na podstawie listy przekazanej przez Zamawiającego;
4) Przypisanie licencji dla poszczególnych użytkowników;
5) Zapewnienie synchronizacji poświadczeń użytkowników z lokalną usługą katalogową Active Directory posiadaną przez Zamawiającego;
6) Zmiana wpisów MX kierujących z obecnego systemu pocztowego, celem przełączenia usługi pocztowej na dostarczone rozwiązanie;
7) Zarchiwizowanie aktualnych skrzynek do lokalnych plików w formacie .pst u 100 użytkowników;
8) Przygotowanie instrukcji zawierającej dane konfiguracyjne dla programów posiadanych przez Zamawiającego: Microsoft Outlook od wersji 2013 i nowszych oraz Mozilla Thunderbird;
9) Wykonanie dokumentacji z przeprowadzonych prac;
10) Prace wdrożeniowe muszą odbyć się po ustaleniu z Zamawiającym harmonogramu wdrożenia, który musi być przedstawiony Zamawiającemu do 4 tygodni od czasu podpisania umowy.

5. Wymagania odnośnie szkolenia

1) Szkolenie musi być realizowane w języku polskim.
2) Szkolenia realizowane będą jako szkolenia zamknięte.
3) Szkolenia muszą odbyć się w siedzibie Zamawiającego.

4) Zamawiający zapewni na potrzeby szkolenia projektor i dostęp do Internet.
5) Szkolący musi zapewnić laptopy do przeprowadzenia szkolenia dla każdego uczestnika szkolenia.
6) Szkolenie musi odbywać się w grupach. Zamawiający deklaruje wskazanie 5 grup szkoleniowych po 20 osób w grupie.
7) Realizujący szkolenie ma obowiązek sprawdzania obecności w trakcie każdego ze szkoleń na podstawie list uczestników przekazanych przez Zamawiającego
8) Szkolenie dla każdej z grup musi mieć związek z wdrożonym rozwiązaniem i dotyczyć: klienta poczty, edytora tekstu, arkusza kalkulacyjnego, edytora prezentacji, klienta poczty w wersji przeglądarkowej, komunikatora, witryn zespołów, dysku w chmurze.
9) Szkolenia mają przybliżać interfejs usług oraz ich obsługę: klient pocztowy w wersji przeglądarkowej, ustawianie autoresponderów, konfiguracji stopki, reguł i przekierowań, udostępniania plików oraz dobrych praktyk przy udostępnianiu i hasłowania adresów URL do dokumentów znajdujących się w usłudze dysku chmurowego, korzystania z komunikatora z uwzględnieniem konfiguracji audio/video, tworzenia spotkań, udostępniania linków spotkań, obsługi czatów, zespołów, grup, udostępniania konwersacji i plików za pośrednictwem komunikatora oraz netykiety, obsługi rozwiązań pakietu internetowego z uwzględnieniem edytora tekstu i arkusza kalkulacyjnego w kontekście pracy zespołowej na pliku, możliwości organizacji pracy na witrynach zespołów – szkolenie poglądowe.
10) Wykonawca ma zapewnić możliwość późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego
11) Wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego materiały dydaktyczne.
12) Wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń.
13) Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń.
14) Wykonawca zobowiązany jest do wystawienia zaświadczenia o odbytym szkoleniu dla każdego uczestnika.

Załącznik nr 1b

Część II

Rozbudowa istniejącego środowiska zarządzania siecią wraz z wdrożeniem rozwiązania NAC

1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1) Dostarczenie oraz wdrożenie systemów kontroli dostępu do sieci NAC
2) Przeprowadzenie szkolenia z wdrożonego rozwiązania dla administratorów systemu

2. **Termin realizacji zamówienia**

Zamawiający wymaga, aby realizacja niniejszego zadania u Zamawiającego, nastąpiła w terminie do 90 dni od dnia podpisania umowy.

3. **Wymagania odnośnie oprogramowania**

1) Z uwagi na aktualnie wykorzystywane rozwiązanie NetSight Suite (ExtremeManagementCenter), Zamawiający wymaga, aby oprogramowanie było uzupełnieniem bądź rozszerzeniem funkcjonalnym aktualnego środowiska, celem zapewnienia jednolitości środowiska i kompatybilności.
2) Zamawiający dopuszcza, aby rozwiązanie NAC zostało wdrożone jako rozwiązanie równoległe bądź zastępujące aktualnie posiadane.
3) Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.

a) Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
b) Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS

4) Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
5) Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami
6) Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
7) Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8) Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9) Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
10) Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11) Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12) Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
13) Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
14) Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.

15) Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
16) Aplikacja musi posiadać wbudowany Syslog serwer.
17) Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
18) Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
19) Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.

a) Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
b) Wysłanie e-mail do wskazanej grupy adresowej
c) Wysłanie informacji SYSLOG do wskazanego serwera
d) Wysłanie TRAP SNMP do wskazanego adresu IP
e) Uruchomienie skryptu w systemie operacyjnym Linux
f) Uruchomienie skryptu skonfigurowanego w systemie zarządzającym

20) Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
21) Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
22) Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23) Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem

a) połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
b) konfiguracji sieci VLAN

24) Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
25) Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:

a) adres IP urządzenia
b) adresu MAC urządzenia
c) nazwy urządzenia
d) wersji oprogramowania
e) wersji bootrom
f) lokalizacji urządzenia
g) danych kontaktowych administratora
h) numeru seryjnego
i) numeru inwentaryzacyjnego – własna numeracja

26) Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:

a) możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
b) możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
c) możliwość odtworzenia wskazanej konfiguracji urządzenia
d) możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
e) możliwość obsługi backup'u urządzeń sieciowych różnych producentów

27) Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie

28) Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
29) Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30) Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
31) Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:

a) przyłączenia do sieci VLAN
b) przyłączenia do serwisu w ramach „Fabric" z wykorzystaniem IEEE 802.1Qcj,
c) konfiguracji Quality of Service
d) konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
e) możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.

32) Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:

a) szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać, gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
b) wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
c) wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
d) generowanie raportów

33) Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.

a) Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
b) Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
c) Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:

- adres IP kontrolera
- liczba obsługiwanych klientów
- szczytowe wartości zajmowanego pasma
- wersja oprogramowania

d) Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:

- adres IP punktu dostępowego
- MAC adres punktu dostępowego
- wersja oprogramowania
- typ punktu dostępowego
- kanały pracy poszczególnych interfejsów radiowych
- szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych

e) Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:

- adres IP klienta
- MAC adres klienta
- nazwa użytkownika
- nazwa punktu dostępowego, do którego dołączony jest użytkownik
- BSSID, do którego dołączony jest użytkownik
- SSID, do którego dołączony jest użytkownik

f) Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:

- zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
- zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
- lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych

34) Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:

a) adresu MAC
b) adresu IP
c) nazwy komputera
d) typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
e) nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
f) adres IP urządzenia, do którego dołączony jest klient.
g) identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
h) typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
i) nazwa przydzielonej polityki bezpieczeństwa.

35) System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.

36) System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa

37) System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:

a) Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
b) Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
c) Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC

d) Realizacji przyłączenia do sieci ze wskazanej „lokalizacji" – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.

e) Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia

38) System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.

39) Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.

40) System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.

41) System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS

42) System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.

43) System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.

44) System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.

45) System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:

a) liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.

b) liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.

c) liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android

d) liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa

e) liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.

46) System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication

47) System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 1 000 urządzeń klienckich (adresów MAC) przez okres minimum 2 lat.

48) System zarządzania musi posiadać przy współpracy z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej

49) Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.

50) Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
51) System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
52) System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
53) Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
54) System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
55) System Analityki musi zapewniać możliwość tworzenia raportów.
56) System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.
57) System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
58) System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
59) System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
60) System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czas
61) System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
62) System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:

a) Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: Palo Alto, Fortinet, Checkpoint
b) Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
c) Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM

63) System zarządzania musi być objęty 12 miesięcznym wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.

4. **Wymagane prace wdrożeniowe**

1) Wypracowanie z Zamawiającym harmonogramu wdrożenia rozwiązania
2) Instalacja rozwiązania na wskazanym przez Zamawiającego zasobie wirtualnym
3) W oparciu o dobre praktyki Zamawiający wymaga od Wykonawcy przedstawienia zalecanych polityk bezpieczeństwa i konfiguracji wskazanego rozwiązania

4) Wykonawca jest zobowiązany do zidentyfikowania urządzeń końcowych pracujących w sieci Zamawiającego i objęcia ich systemem NAC w ramach dostarczonej licencji
5) Uruchomienie NAC w trybie monitoringu
6) Objęcie systemem NAC aktualnie stosowanych przez Zamawiającego przełączników sieciowych marki Extreme Networks oraz urządzenia UTM marki Fortinet Fortigate
7) Wymagane jest przeprowadzenie testów powdrożeniowych w zakresie wdrożonych polityk i stabilności pracy systemu
8) Wykonawca zobligowany jest do utworzenia i dostarczenia dokumentacji powdrożeniowej Zamawiającemu z wykonanych prac
9) Wymagane jest przeprowadzenie szkolenia zdalnego lub w siedzibie Zamawiającego w liczbie minimum 8h z wdrożonego rozwiązania z zakresu: obsługi interfejsu, administracji, weryfikacji logów zdarzeń oraz tworzenia polityk (szkolenie dla 2 administratorów)
10) Zamawiający przed wykonaniem szkolenia przez Wykonawcę musi zaakceptować ramowy plan szkolenia przedstawiony na minimum 14 dni przed planowanym terminem przeprowadzenia szkolenia
11) W przypadku szkolenia w siedzibie Zamawiającego, Zamawiający zapewnieni odpowiednie warunki do przeprowadzenia szkolenia – dedykowane pomieszczenie i projektor.
12) Wykonawca zobowiązany jest do wystawienia zaświadczenia o odbytym szkoleniu dla każdego uczestnika.