**Załącznik nr 1 do opisu przedmiotu zamówienia**

**PROGRAM FUNKCJONALNO-UŻYTKOWY**

Zaprojektowanie i rozbudowa infrastruktury sieci komputerowych z wdrożeniem wewnętrznej infrastruktury sieciowo – usługowej w Szkołach Podstawowych Miasta Ostrołęka

**Kod główny zamówienia CPV:**

32420000-3 Urządzenia sieciowe

**Kody pomocnicze zamówienia CPV:**

32413100-2 Rutery sieciowe,

32421000-0 Okablowanie sieciowe,

324240000-1 Infrastruktura sieciowa,

45310000-3 Roboty w zakresie okablowania strukturalnego,

48820000-2 Serwery.

**Zamawiający: Miasto Ostrołęka**

**Ostrołęka**, **lipiec 2019 roku**

I. Opis ogólny przedmiotu zamówienia 3

I. 1 Założenia i szczegółowy opis zadania 3

II. Budowa kablowej sieci LAN 4

II.1 Normy 4

II.2 Założenia ogólne dla okablowania strukturalnego 5

II.2.1 Struktura okablowania 5

II.2.2 Graniczne długości 6

II.2.3 Wymagania dotyczące okablowania strukturalnego 6

II.2.4 Trasy kablowe 7

II.3 Wymagania szczegółowe dla komponentów okablowania strukturalnego 8

II.3.1 Specyfikacja kabla instalacyjnego 8

II.3.2 Specyfikacja panelu krosowego 9

III. Urządzenia aktywne sieci okablowania strukturalnego. 10

III.1 Wymagania minimalne dla zapory ogniowej Firewall/Router 10

III. 2 Wymagania minimalne dla przełącznika sieciowego 15

III.3 Wymagania minimalne dla punktu dostępowego WiFi 17

III.4 Wymagania minimalne dla serwera multimedialnego NAS 18

IV. wykonania i odbioru robót 19

# I. OPIS OGÓLNY PRZEDMIOTU ZAMÓWIENIA

## **I. 1 Założenia i szczegółowy opis zadania**

 Celem opracowania jest opis ilościowo-jakościowy przedmiotu zamówienia. Niniejsze opracowanie służy również przygotowaniu oferty w ramach postępowania przetargowego zgodnie z przepisami zamówień publicznych.

 Zadaniem polegającym na rozbudowanie infrastruktury sieciowo – usługowej objęte są następujące szkoły w Mieście Ostrołęka:

1. Szkoła Podstawowa Nr 2 im. Stanisława Staszica, ul. Papiernicza 1,

2. Szkoła Podstawowa Nr 4 ul. Legionowa 17,

3. Szkoła Podstawowa Nr 5 im. Zofii Niedziałkowskiej, ul. Hallera 12,

4. Szkoła Podstawowa Nr 6 im. Orła Białego, ul. Sienkiewicza 15,

5. Szkoła Podstawowa Nr 10 im. Jana Pawła II, ul. Blachnickiego 16.

 Przedmiot zamówienia obejmuje zaprojektowanie i wykonanie:

* sieci okablowania strukturalnego poziomego - 105 gniazd 1xRJ45 (po 21 punktów RJ-45
w każdej z 5 szkół podstawowych),
* dostawy i wdrożenia punktów dostępowych sieci WiFi – 105 szt. (po 21 szt. w każdej z 5 szkół podstawowych) ,
* szaf teleinformatycznych 19” wraz z zasilaniem, wyposażonych w panele krosowe sieci miedzianej 24xRJ45 - min. 5 kpl. ,
* Głównych Punktów Dystrybucyjnych (GPD) i dodatkowych (jeżeli zajdzie potrzeba) Pośrednich Punktów Dystrybucyjnych (PPD) sieci LAN w każdej z 5 szkół podstawowych w miejscach wskazanych przez umocowanych przedstawicieli szkół – min. 5 kpl., każdy składający się z:

a) zapory ogniowej (Firewall) chroniącej komputerowe sieci szkolne przez zagrożeniami sieci Internet;

b) zestawu przełączników dostępowych w punktach GPD i/lub PPD o łącznej ilości 24 portów aktywnych. Każdy zestaw składa się z dwóch przełączników min. 12 portowych, których montaż odbywa się tylko w GPD lub po jednym w GPD i w PPD - zależy od potrzeb projektowych;

c) serwera multimedialnego NAS wraz z uruchomieniem oraz wstępną konfiguracją serwerów pod przyszłe usługi cloudowe umożliwiające przetwarzanie i udostępnianie kontentu dydaktyczno-edukacyjnego pomiędzy szkołami oraz budowanie zasobów edukacyjnych w szkołach, które będzie można zapisywać, synchronizować i udostępniać pomiędzy szkołami z dowolnego miejsca i w dowolnym czasie na serwerach NAS;

Wymagania minimalne dla poszczególnych urządzeń zostały przedstawione w niniejszym dokumencie.

 Wykonawca w celu dokładnego skalkulowania kosztów budowy infrastruktury kablowo-zasilającej sieci LAN powinien odbyć wizję lokalną, poprzedzającą złożenie oferty
w postępowaniu przetargowym. Załącznikiem do PFU są wykazy planowanego rozmieszczenia punktów dostępowych sieci WiFi na terenie szkół, w postaci wizualizacji miejsc ich rozmieszczenia ma planach kondygnacji szkół objętych projektem.

 Na wizji lokalnej zostaną wskazane miejsca/sale, w których należy zapewnić dostęp do Internetu.

 Istniejące sieci komputerowe w szkołach zostaną włączone do nowych urządzeń Firewall/ Router w sposób niezależny od nowobudowanych. Niezbędną rekonfigurację sieci istniejących wykonają przedstawiciele szkół.

# II. BUDOWA KABLOWEJ SIECI LAN

 W ramach zadania Wykonawca musi wybudować w każdej szkole 21 Punktów Logicznych (PL) rozumianych jako 1 x RJ45, w miejscach ustalonych z Zamawiającym. Łącznie 105 punktów logicznych PL (1x RJ45).

 Okablowanie należy wykonać w kat. 5e nieekranowej z użyciem kabla U/UTP kat. 5e LSOH 200 MHz. Kable po stronie Głównego Punktu Dystrybucyjnego (GPD), Pośredniego Punktu Dystrybucyjnego (PPD) należy zakończyć na nieekranowanych patchpanelach kat. 5e.

W celu ułożenia i dystrybucji wymaganego okablowania LAN na terenie szkoły, Wykonawca może wykorzystać istniejące trasy kablowe, pod warunkiem ich drożności i możliwości ułożenia w nich wymaganego okablowania LAN. W przeciwnym razie Wykonawca musi wybudować nowe trasy kablowe zapewniające ułożenie wymaganej ilości kabli sieci LAN do miejsc montażu punktów dostępowych sieci bezprzewodowej WiFi.

 Wykonawca w celu dokładnego skalkulowania kosztów budowy infrastruktury kablowo-zasilającej sieci LAN powinien odbyć wizję lokalną, poprzedzającą złożenie oferty. Na wizji lokalnej zostaną wskazane miejsca/sale, w których należy zapewnić dostęp do Internetu.

## **II.1 Normy**

 Przedmiotem zadanie jest wybudowanie instalacji okablowania strukturalnego LAN
w trybie zaprojektuj i wybuduj. Dokumentację należy opracować zgodnie ze wskazówkami
i zaleceniami Zamawiającego, z uwzględnieniem elastyczności systemu oraz wymagań nowoczesnych urządzeń transmisji danych.

 Podstawą do opracowania zagadnień związanych z okablowaniem strukturalnym są normy okablowania strukturalnego.

 Normy europejskie dotyczące okablowania strukturalnego – wymagań ogólnych
i specyficznych dla danego środowiska:

* *ISO/IEC11801: 2011 - Information technology - Generic cabling for customer premises*
* *PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego - Część 1: Wymagania ogólne*
* *PN-EN 50173-2:2008/A1:2011E Technika Informatyczna – Systemy okablowania strukturalnego - Część 2: Budynki biurowe;*

Normy europejskie pomocnicze - w zakresie instalacji:

* *PN-EN 50174-1:2010/A1:2011E Technika informatyczna. Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości;*
* *PN-EN 50174-2:2010/A1:2011E Technika informatyczna. Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;*
* *PN-EN 50174-3:2014-02 Technika informatyczna. Instalacja okablowania -Część 3 - Planowanie i wykonawstwo instalacji na zewnątrz budynków;*
* *PN-EN 50346:2004/A2:2010P Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania*
* *PN-EN 50310:2016-09 Sieci połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi*

 W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.

 Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami norm obowiązujących w czasie realizacji zadania, przy uwzględnieniu wszystkich wymagań opisanych w dokumentacji projektowej a zdefiniowane przez dokumenty wskazane powyżej.

 System okablowania oraz wydajność komponentów na etapie oddania instalacji do użytku musi pozostać w zgodzie z wymaganiami norm PN-EN50173-1:2011
i ISO/IEC11801:2011.

## **II.2 Założenia ogólne dla okablowania strukturalnego.**

### II.2.1 Struktura okablowania

 Z uwagi na rozległą strukturę użytkowanego obiektu, zakłada się, że instalacja okablowania strukturalnego wykonana zostanie w oparciu o topologię hierarchiczną. Schemat hierarchicznej struktury sieci strukturalnej przedstawia rysunek 1.



Rysunek 1 Schemat topologii hierarchicznej okablowania strukturalnego

 Zakłada się, że system okablowania strukturalnego składać się będzie z trzech sektorów zgodnych z normą europejską EN50173-1:

1. Okablowanie szkieletowe (pionowe) w przypadku wybudowania Pośrednich Punktów Dystrybucyjnych (PPD),

2. Okablowanie poziome,

3. Okablowanie obszaru roboczego, kable zakończone złączem RJ-45 do podłączenia punktów dostępowych sieci WiFi.

 Na potrzeby niniejszego opracowania, przyjęto oznaczenia:

* GPD – Główny Punkt Dystrybucyjny, szafa 19” wyposażona w elementy pasywnei aktywne systemu okablowania strukturalnego, będąca centralnym punktem sieci okablowania strukturalnego. Od GPD rozchodzi się instalacja okablowania poziomego do punktów logicznych.
* PPD – Pośredni Punkt Dystrybucyjny, szafa 19” obsługująca dany obszar roboczy, w której znajdują się elementy aktywne i pasywne systemu okablowania strukturalnego. Od PPD rozchodzi się instalacja okablowania poziomego do punktów logicznych.
* PL – Punkt Logiczny 1 x RJ-45 zakończenie okablowania poziomego w postaci złącza RJ45, będące punktem przyłączeniowym dla urządzeń końcowych punktów dostępowych sieć WiFi.

### II.2.2 Graniczne długości

 Długość łącza stałego (permanent link) okablowania strukturalnego, tj. odległość pomiędzy złączem RJ45 w PL a złączem RJ45 w patchpanelu po stronie punktu dystrybucyjnego (GPD/PPD), nie może przekroczyć 90 m.

 Kabel przyłączeniowy od PL do urządzenia końcowego (punktu dostępowego WiFi), nie może przekroczyć dł. 5m. Podobnie kabel krosowy w GPD/PPD, pomiędzy patchpanelem
a urządzeniem aktywnym (przełącznikiem sieciowym), nie może przekroczyć dł.5m. Całość łącza z okablowaniem szafowym oraz okablowaniem obszaru roboczego, czyli kanał (channel), nie może w sumie przekroczyć 100 m.

### II.2.3 Wymagania dotyczące okablowania strukturalnego

 Wymagania i główne założenia dotyczące systemu okablowania strukturalnego:

* Wszystkie komponenty systemu okablowania mają być zgodne z wymaganiami obowiązujących norm wg.:

- ISO/IEC 11801,

- EN 50173-1,

- ANSI/TIA/EIA 568-C.2

* Producent oferowanego systemu okablowania strukturalnego musi spełniać najwyższe wymagania w zakresie zarządzania potwierdzone następującymi certyfikatami: ISO 9001.
* W obiekcie projektuje się instalację teletechniczną, która wykonana będzie jako nieekranowana sieć okablowania strukturalnego klasy D (komponenty min. kategorii 5e), poprowadzona kablem o paśmie przenoszenia min. 200MHz. Konstrukcja kabla pozwala osiągnąć wysokie parametry transmisyjne, oraz zmniejszyć przesłuchy NEXT i PSNEXT oraz zmniejszenie przesłuchów obcych Alien Crosstalk. Kabel musi spełniać wymagania stawiane komponentom przez najnowsze normy.
* Ilość Punktów Logicznych (PL) oraz punktów dystrybucyjnych GPD/PPD przyjęto na podstawie aktualnych, na dzień sporządzenia programu funkcjonalno-użytkowego wytycznych Zamawiającego i istniejącej aranżacji wnętrz, w których mają znaleźć się punkty GPD/PPD. W przypadku zmiany koncepcji, ostateczna i precyzyjna lokalizacja gniazd logicznych powinna być ustalona między Użytkownikiem, a Wykonawcą w trakcie realizacji.

### II.2.4 Trasy kablowe

 W celu ułożenia i dystrybucji wymaganego okablowania LAN na terenie szkoły, Wykonawca może wykorzystać istniejące trasy kablowe, pod warunkiem ich drożności
i możliwości ułożenia w nich wymaganego okablowania LAN. W przeciwnym razie Wykonawca musi wybudować nowe trasy kablowe zapewniające ułożenie wymaganej ilości kabli sieci LAN do miejsc montażu punktów dostępowych sieci bezprzewodowej WiFi.

 Projektując i wykonując trasy dla kabli logicznych uwzględniono konstrukcję budynku oraz bezkolizyjność z innymi instalacjami i urządzeniami; trasa powinna przebiegać wzdłuż linii prostych równoległych i prostopadłych do ścian i stropów zmieniając swój kierunek tylko w zależności od potrzeb (tynki, rozgałęzienia, podejścia do urządzeń), trasa przebiegu powinna być przy tym łatwo dostępna do konserwacji i remontów, a jej wytyczanie powinno uwzględniać miejsca mocowania konstrukcji wsporczych instalacji. Należy przestrzegać utrzymania jednakowych wysokości zamocowania wsporników i odległości między punktami podparcia.

- Maksymalna długość kabla instalacyjnego skrętkowego (od punktu dystrybucyjnego do gniazda końcowego) nie może w żadnym przypadku przekroczyć 90 metrów.

- Okablowanie powinno być ciągłe na całej długości toru bez złącz i spawów od stanowiska roboczego do panelu rozdzielczego.

- Wszystkie cztery pary każdego kabla powinny być zakończone w pojedynczym module.

- Wymaga się standardowej sekwencji połączeń T568A lub T568B.

- Proces montażu ma gwarantować najwyższą powtarzalność. Maksymalny rozplot pary transmisyjnej na złączu modularnym RJ45 nie może być większy niż 6 mm.

- Każdy kabel powinien mieć trwałe oznaczenie na dwóch końcach przy zakończonych modułach wg przyjętego systemu numeracji.

- Każdy stelaż szafy powinien być podłączony do listwy uziemiającej zgodnie z wymogami norm.

- Odpowiednie bariery ogniowe powinny być zastosowane dla kabli przechodzących przez ściany i przegrody stanowiące rozdzielnie stref ogniowych budynku. Nieużywane szachty
i piony technologiczne powinny być zabezpieczone przed przenikaniem ognia.

- Instalacja powinna być przeprowadzona w sposób profesjonalny używając do tego celu najlepszych urządzeń i narzędzi oraz korzystając z instalatorskiego doświadczenia.

- Wszystkie instalowane kable powinny być poprawnie umieszczone w rurkach kablowych, na drabinkach kablowych, w rynienkach lub w kanałach instalacyjnych. Jeśli zastosowanie elementów ochronnych dla medium transmisyjnego jest niemożliwe, pojedyncze kable mogą być formowane w wiązki, starannie prowadzone, poprawnie osłonięte, przymocowane
i zabezpieczone za pomocą opasek kablowych do konstrukcji nośnej budynku.

- Okablowanie powinno być prowadzone w sposób uporządkowany i zgodnie z wytycznymi producenta. Wszystkie używane opaski kablowe powinny być rzepowe i ręcznie zaciskane tylko w punktach gdzie nie ma zagięć i skręceń.

- Jeśli używana jest rurka osłonowa, maksymalna liczba zagięć większych niż 90º między punktami przeciągania nie powinna przekraczać 2.

- Wszystkie kable światłowodowe i miedziane powinny być instalowane i mocowane zgodnie z wytycznymi producenta. Podczas układania kabli instalator powinien dbać o to, aby kabel nie był narażony na nacisk i zagięcia.

- Po instalacji kabla, instalator powinien się upewnić, że wszystkie części kabla są prawidłowo zamocowane i nie ma żadnych naprężeń wzdłuż drogi prowadzenia kabla i na jego końcach.

- Szczególną uwagę należy zachować przy układaniu kabli kat. 5e, aby zachować ich promień gięcia zgodnie z wytycznymi producenta kabli. Kable kat. 5e nie powinny mieć mniejszego promienia zgięcia niż 8x średnica kabla podczas instalacji i 4x średnica kabla podczas eksploatacji.

Główne i Pośrednie Punkty Dystrybucyjne (GPD i PPD).

 Dla Głównych i Pośrednich Punktów Dystrybucyjnych projektuje się szafy wiszące RACK 19” o wysokościach od 6U do 12U, przeznaczone do montażu okablowania LAN
i urządzeń aktywnych sieci Wifi. Szafa musi mieć konstrukcję skręcaną i być dostępna w wersji zmontowanej bądź do samodzielnego montażu. Szafa musi być wyposażona w podwójny stelaż 19” (z przodu i z tyłu). Wymagana nośność szafy to minimum 60kg. Aby zapewnić elastyczność instalacji wymaga się aby szafa posiadała możliwość wyprowadzenia kabli z góry z dołu i od tyłu, zdejmowane osłony boczne, zamykane na zamek. W celu zapewnienia właściwej sztywności szafy i stabilności montażu szafa musi posiadać ścianę tylną. Szafa powinna możliwość zmiany strony mocowania drzwi.

 Szafa teleinformatyczna powinna być wyposażona:

* w dedykowany panel wentylacyjny dachowy (2 wentylatorowy),
* listwę kablową zasilającą (min. 6 gniazd 230 VAC), wykonanie zasilania listwy
z istniejących obwodów leży po stronie Wykonawcy.

 Wymagana głębokość szafy min. 500 mm.

## **II.3 Wymagania szczegółowe dla komponentów okablowania strukturalnego**

### II.3.1 Specyfikacja kabla instalacyjnego

 Należy zastosować kabel kat. 5e o konstrukcji U/UTP (kabel nieekranowany). Minimalne wymagania elementów okablowania strukturalnego to kategoria 5e (komponenty) /Klasa D (wydajność całego systemu).

 Kabel musi spełniać wymagania poniższych norm:

- PN-EN 50173-1:2013

- EN 50173-1:2011

- ISO/IEC 11801 Edition 2.2

- ANSI/TIA-568-C.0

- ANSI/TIA-568-C.1

- ANSI/TIA-568-C.2

- IEC 60754-2

 Do każdego punktu logicznego zakończonego złączem RJ-45 należy doprowadzić kabel skrętkowy 4-parowy. Każdy kabel skrętkowy, 4-parowy należy zakończyć na pojedynczym module RJ45 (gnieździe RJ45) po stronie panelu krosowego. Nie dopuszcza się rozdziału jednego kabla 4-parowego na większą ilość portów (nie dopuszcza się wkładek i przejściówek rozdzielających). Ze względu na przyjęte wymiary przepustów kablowych oraz zaprojektowane trakty prowadzenia kabli i związane z tym prześwity, wymagane jest zastosowanie medium transmisyjnego o maksymalnej średnicy zewnętrznej 5,2mm. Nie dopuszcza się kabli
o większej średnicy zewnętrznej. Kabel ten ma zapewniać pozytywne parametry transmisyjne w całym paśmie minimum 200MHz. Projektowany kabel musi posiadać zewnętrzną powłokę LSOH nie wydzielającą szkodliwych toksyn podczas spalania. Wymaga się, aby kabel posiadał euroklasę Dca s2,d2,a1 zgodnie z dyrektywą CPR.

 Wymagania minimalne dla kabla:

* Konstrukcja U/UTP
* Powłoka bezhalogenowa.
* Zgodny z kategorią 5e
* Znacznik długości od 305 do 0, co 1m.
* Testowany do 200 MHz
* Powłoka zewnętrzna: LSOH
* Średnica zewnętrzna: max 5,2 mm
* Średnica przewodnika: 24 AWG
* Euroklasa Dca- s2,d2,a1

 Wymaga się, aby wewnątrz kabla znajdował się separator rozdzielający pary w kablu. Separator odpowiada ze utrzymanie odpowiedniej pozycji par i ich odległości względem siebie, eliminując przesłuchy wewnątrz kabla. Podczas instalacji należy pamiętać o odpowiednich promieniach gięcia kabla. Instalacja ze zbyt małym promieniem gięcia kabla może doprowadzić do pogorszenia właściwości transmisyjnych w torze.

### II.3.2 Specyfikacja panelu krosowego

 Kable należy zakończyć na nieekranowanych panelach kategorii 5e.

 Panel musi spełniać wymagania kategorii 5e (klasy D) wg poniższych norm:

- PN-EN 50173-1:2013

- EN 50173-1:2011

- ISO/IEC 11801 Edition 2.2

- ANSI/TIA-568-C.0

- ANSI/TIA-568-C.1

- ANSI/TIA-568-C.2

 Panel powinien posiadać 24 porty i wysokość 1U. W celu zapewnienia Użytkownikowi optymalnych parametrów instalacyjnych i serwisowych, projektuje się patchpanele oparte
o system wymiennych płytek PCB ze złączami szczelinowymi IDC LSA+ ustawionymi pod kątem 45 stopni. Na jednej płytce powinno znajdować się nie więcej niż 8 portów RJ45. Złącze szczelinowe powinno posiadać oznaczenia kolorystyczne ułatwiające przyłączenie kabla
w sekwencji 568B lub 568A. Panel musi posiadać zintegrowaną prowadnicę kabli przychodzących, co zapewni swobodne uchwycenie kabli i eliminacje naprężeń związanych
z wagą doprowadzonych kabli. Ponad to panel musi być oznaczony logo wybranego producenta. Wraz z panelem musi być dostarczony komplet elementów mocujących kable do panelu tj. opaski kablowe plastikowe. Patchpanel musi być wyposażony w gwintowane przyłącze linki uziemienia panelu. Wszystkie zainstalowane panele muszą być podłączone poprzez ww. przyłącze do szyny uziemienia szafy.

# III. URZĄDZENIA AKTYWNE SIECI OKABLOWANIA STRUKTURALNEGO

### III.1 Wymagania minimalne dla zapory ogniowej Firewall/Router.

**PARAMETRY SPRZĘTOWE**

1. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
2. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci Flash.
3. Liczba portów Ethernet 10/100/1000Mbps – min. 8.
4. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta.
5. Przepustowość Firewalla – min. 3,3 Gbps.
6. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,3 Gbps.
7. Przepustowość filtrowania Antywirusowego – min. 350 Mbps.
8. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 500 Mbps.
9. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100.
10. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 18.
11. Obsługa min. VLAN 64.
12. Liczba równoczesnych sesji - min. 280 000 i nie mniej niż 15 000 nowych sesji/sekundę.
13. Urządzenie jest nielimitowane na użytkowników.

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
6. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u.
7. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
8. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu
i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych
i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu
w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika
o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP
i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSPAM

1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
	1. białe/czarne listy,
	2. DNS RBL,
	3. heurystyczny skaner.
3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.

WIRTUALNE SIECI PRYWANTE (VPN)

1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Odpowiednio kanały VPN można budować w oparciu o:
	1. PPTP VPN,
	2. IPSec VPN,
	3. SSL VPN
3. SSL VPN musi działać w trybach Tunel i Portal.
4. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN
współpracującego z oferowanym rozwiązaniem.
5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator musi mieć możliwość dodawania własnych kategorii URL.
4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:

a) blokowanie dostępu do adresu URL,

b) zezwolenie na dostęp do adresu URL,

c) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

1. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron
z komunikatem o zablokowaniu strony.
2. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
3. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
4. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych
z wykorzystaniem typu MIME.
5. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
6. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

UWIERZYTELNIANIE

1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników
w oparciu o:

a) lokalną bazę użytkowników (wewnętrzny LDAP),

b) zewnętrzną bazę użytkowników (zewnętrzny LDAP),

c) usługę katalogową Microsoft Active Directory.

1. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
2. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia
autoryzacje w oparciu o protokoły:

a) SSL,

b) Radius,

c) Kerberos.

1. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
2. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
3. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu
o następujące dwa mechanizmy:

a) równoważenie względem adresu źródłowego,

b) równoważenie względem połączenia.

1. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
2. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
4. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
5. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu
w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
6. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej
o protokoły: RIPv2, OSPF oraz BGP.

**POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA**

1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
6. Urządzenie musi posiadać usługę DNS Proxy.

**ADMINISTRACJA URZĄDZENIEM**

1. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
2. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
3. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową
a komunikacja musi być zabezpieczona za pomocą protokołu https.
4. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
5. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
6. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
7. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
8. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
9. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
10. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
11. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

**RAPORTOWANIE**

1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania
i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów.
5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania
z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

**SERWISY I LICENCJE**

 W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować wszystkie wymagane funkcjonalności ochronne na okres 36 miesięcy.

**GWARANCJA I WSPARCIE**

 Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres
36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

### III. 2 Wymagania minimalne dla przełącznika sieciowego

1. Przełącznik o wysokości 1U posiadający 12 portów 10/100/1000BaseT PoE+ (RJ45)
oraz min. 2 porty 100/1000BASE-X (SFP); zgodny z IEEE 802.3at - PoE+ Power
over Ethernet;
2. Wbudowany dodatkowy port Ethernet do zarządzania poza pasmem - out of band management;
3. Budżet mocy dla technologii PoE – min. 120W;
4. Zgodność ze standardem IEEE 802.3az - Energy Efficient Ethernet dla portów 10/100/1000Base-T;
5. Szerokość przełącznika umożliwiająca montaż dwóch urządzeń obok siebie w jednym rzędzie szafy typu RACK 19”;
6. Przełącznik musi posiadać wbudowany zasilacz 230V AC;
7. Maksymalny pobór mocy urządzenia 162W;
8. Możliwość pracy w trybie pasywnego chłodzenia (przy wyłączonych wentylatorach)
w temperaturze poniżej 35 °C;
9. Nieblokującą architekturę o wydajności przełączania min. 28Gb/s;

10 Szybkość przełączania min. 20 Milionów pakietów na sekundę;

11 Tablica MAC adresów min. 16k;

12 Pamięć operacyjna: min. 512MB pamięci DRAM;

13 Pamięć flash: min. 128MB pamięci Flash;

14 Pojemność bufora pakietów min. 1,5MB;

15 Obsługa sieci wirtualnych IEEE 802.1Q – min. 1024; Quality of Service: IEEE 802.1p; DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym.

16 Wsparcie dla ramek Jumbo;

17 Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB; LLDP Media Endpoint Discovery (LLDP-MED); protokołu UDLD;

18 Routing statyczny - min. 60 wpisów; Klient SSH2;

19 Obsługa Multicast VLAN Registration – MVR; IGMP snooping; TACACS+; Guest VLAN dla IEEE 802.1x; protokołu GVRP lub równoważnego odpowiadającego za dynamiczną propagacje VLAN;

20 Wsparcie dla IEEE 802.3x; IEEE 802.1x; sFlow; RFC3580; RSPAN

21 Obsługa funkcjonalności monitoringu pakietów i protected ports; RADIUS Authentication (RFC 2865); RADIUS Accounting (RFC 2866);

22 Bezpieczeństwo MAC adresów: zatrzaśnięcie MAC adresu na porcie oraz przypisania statycznych MAC adresów do portu.

23 Minimum 100 list kontroli dostępu (ACL) z min. 1000 reguł każda, bazujących co najmniej na poniższych kryteriach: Time-Based ACL, Źródłowy/Docelowy adres IP, Źródłowy/Docelowy port TCP/UDP, Typ protokołu IP, Type of Service (ToS) lub pole DSCP, Źródłowy/Docelowy adres MAC, EtherType, IEEE 802.1p, VLAN ID.

24 Obsługa bezpiecznego transferu plików SCP (Secure Copy);

25 Obsługa DHCP Snooping; STP (Spinning Tree Protocol) IEEE 802.1d; RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w; MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s; STP Loop/Root Guard; Link Aggregation IEEE 802.3ad – min, 6;

26 Obsługa synchronizacji czasu SNTP (Simple Network Time Protocol); SYSLOG;

27 Obsługa RMON min. 4 grupy: Statistics, History, Alarms, Events;

28 Minimalny zakres temperatur pracy 0°C do 50°C.

29 Zarządzanie przez interfejs CLI, przeglądarkę WWW – protokół http i https;

30 Zarządzanie przez SNMP v1/v2/v3;

31 Obsługa skryptów CLI;

32 Możliwość zarządzania z poziomu dostarczanego przez producenta oprogramowania do zarządzania infrastrukturą sieciową:

a) w formie systemu instalowanego w sieci wewnętrznej Zamawiającego,

b) w formie usługi chmurowej (chmura publiczna).

33 Możliwość konfiguracji nowego urządzenia za pomocą wzorców konfiguracji pobieranych
z oprogramowania do zarządzania infrastrukturą sieciową – zarówno w wersji instalacyjnej (sieć LAN Zamawiającego), jak i w wersji chmurowej;

34 Dożywotnia gwarancja producenta uwzględniająca:

a) wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,

b) aktualizację oprogramowania układowego (firmware),

c) wsparcie techniczne producenta przez telefon, e-mail oraz serwis www przez okres
min. 36 miesięcy,

d) dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.

### III.3 Wymagania minimalne dla punktu dostępowego WiFi

 W ramach zadania zakłada się, iż funkcję kontrolera sieci bezprzewodowej WiFi
w każdej szkole, będzie pełnił 1 AP WiFi.

 Z uwagi na zarządzanie siecią bezprzewodową WiFi z jednego centralnego miejsca, przełączniki sieci aktywnej oraz urządzenia sieci bezprzewodowej WiFi powinny być tego samego producenta.

1. Musi pracować z trybach pracy niezależnej (Standalone) oraz pracy z kontrolerem WLAN oraz zarządzać pracą pozostałych AP WiFi w danej grupie;
2. Musi być wyposażony w 2 moduły radiowe z obsługą 2,4GHz i 5GHz oraz moduł Bluetooth (BLE) oraz posiadać wbudowane anteny min. 4,5dBi dla 2,4GHz oraz 7,5dBi dla GHz;
3. Musi posiadać dwa moduły radiowe obsługujące standardy IEEE 802.11a/b/g/n/ac;
4. Musi posiadać min. 2 interfejsy sieciowe IEEE 802.3 Gigabit Ethernet; możliwość zasilania innych urządzeń końcowych z interfejsu punktu dostępowego (wsparcie dla PoE-Out);
5. Musi obsługiwać 2x2 MIMO z modulacją 256-QAM w obu zakresach częstotliwości (2.4GHz i 5GHz) oraz 8 SSID per moduł radiowy (16 per AP);
6. Możliwość zasilania PoE (Power-over-Ethernet) ze wsparciem dla standardów IEEE 802.3af oraz IEEE 802.3at oraz mieć możliwość zasilania z zewnętrznego zasilacza 12 DC;
7. Musi realizować pracę z pełną wydajnością przy zasilaniu PoE zgodnie z IEEE 802.11af;
8. Musi pracować w trybie punktu dostępowego lub sensora WIPS (wbudowany IDS oraz sensor WIPS);
9. Musi posiadać funkcjonalność równomiernego dystrybuowania klientów pomiędzy punktami dostępowymi i pasmami częstotliwościowymi;
10. Musi wspierać standard 802.11r Fast Roaming oraz mechanizm wykrywający zakłócenia
 i automatycznie dostosowywać do nich kanał pracy oraz moc sygnału;
11. Musi umożliwiać konfigurowanie routingu L3 oraz NAT oraz konfigurację 802.1x, 802.11i, WPA, WPA2;
12. Musi być wyposażony w firewall typu stateful; umożliwiać filtrowanie IP;
13. Musi zapewniać dostęp poprzez usługi Dynamic DNS oraz uruchomienie serwera DHCP;
14. Musi realizować usługę serwera RADIUS i usługę klienta VPN; oraz realizować QoS – min. WMM, WMM-UAPSD, 802.1p, Diffserv i TOS;
15. Musi posiadać wbudowanego klienta tunelu L2TPv3 oraz IPsec oraz wbudowaną widoczność i kontrola aplikacji w oparciu o DPI (Deep Packet Inspection);
16. Musi wykorzystywać usługi lokalizacyjne do określenia położenia klientów sieci WLAN,
 a także kontroli dostępu do sieci i aplikacji;
17. Musi umożliwiać uruchomienie usługi hot-spot oraz mieć możliwość uruchomienia usługi dostępu gościnnego (Captive Portal);
18. Musi być wyposażony w diody LED sygnalizujące stan pracy każdego z modułów radiowych;
19. Musi posiadać certyfikat kompatybilności WiFi Alliance;
20. Temperatura pracy w zakresie od 0° C do min. 40° C.
21. Gwarancja min. 3 lata.

### III.4 Wymagania minimalne dla serwera multimedialnego NAS

|  |  |  |
| --- | --- | --- |
| **Lp.**  | **Parametr**  | **Wymagania minimalne** |
| 1. | Procesor, Pamięć RAM | Procesor o taktowaniu nie mniejszym niż 1,4GHz 64-bitowy, min. 4 rdzenie, min. 2GB DDR4 |
| 2. | Obudowa | RACK 19" |
| 3. | Liczba zatok na dyski twarde | Min. 4 |
| 4. | Obsługiwane dyski twarde | 3.5" oraz 2.5" SATA |
| 5. | Dyski | przedmiot dostawy obejmuje 2 dyski 4TB SATA  |
| 6. | Możliwość podłączenia modułu rozszerzającego | Tak |
| 7. | Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż: | 8 |
| 8. | Porty na karty rozszerzeń | 1 x Gen2 x8 PCIe |
| 9. | Porty LAN 1GbE RJ45 | min. 4 |
| 10. | Port eSATA | min. 1 |
| 11. | Porty USB 3.0 | min. 2 |
| 12. | Zasilanie | Zasilacz o mocy maks. 100W |
| 13. | Sprzętowe szyfrowanie wolumenów | Tak |
| 14. | Wewnętrzny system plików | BTRFS, EXT4 |
| 15. | Obsługiwane tryby RAID | JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| 16. | Funkcje backup | Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows, serwer Apple Time Machine, backup na zewnętrzne dyski twarde,  |
| 17. | Darmowe aplikacje na urządzenia mobilne | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Dostępne na systemy iOS oraz Android |
| 18. | Minimum obsługiwane aplikacje/usługi | Serwer plików, Serwer FTP, Serwer WEB, Serwer kopii zapasowych, Serwer wydruku, Narzędzia do pracy grupowej dostępne przez przeglądarkę WWW (Edytor tekstu, Arkusz kalkulacyjny, Chat) dostarczane przez producenta urządzeniaSerwer Monitoringu (opcja podłączenia 2 kamer IP z możliwością podłączenia dodatkowych, do min. 30 kamer) |
| 19. | VPN | VPN Server |
| 20. | Certyfikaty | FCC Class A, CE Class A, BSMI Class A, EAC, VCCI, CCC, RCM |
| 21. | Gwarancja producenta | Min. 3 lata, także na dyski |

# IV. WARUNKI WYKONANIA I ODBIORU ROBÓT

 Zamawiający przewiduje bieżącą kontrolę realizacji zamówienia. Szczególnym przedmiotem oceny będzie zgodność przyjętych rozwiązań i materiałów z podpisaną umową, niniejszym opracowaniem, a także obowiązującymi przepisami i normami.

 Na Wykonawcy spoczywa obowiązek zapewnienia odpowiednio wykwalifikowanego personelu niezbędnego do prawidłowego zaprojektowania i wykonania przedmiotu zamówienia.

 Wykonawca winien dysponować:

* co najmniej jedną osobą, która będzie pełnić funkcję Specjalisty ds. zabezpieczeń sieci, posiadającą doświadczenie polegające na udziale w co najmniej dwóch zadaniach, które swoim zakresem obejmowały wdrożenie systemów bezpieczeństwa sieciowego oraz ważny certyfikat potwierdzający wiedzę i umiejętności we wdrażaniu rozwiązania zaoferowanego przez Wykonawcę, wystawiony przez producenta systemu lub dystrybutora lub autoryzowany ośrodek certyfikujący;
* co najmniej jedną osobą, która będzie pełnić funkcję Specjalisty ds. sieci aktywnych, posiadającą doświadczenie polegające na udziale w co najmniej dwóch zadaniach, które swoim zakresem obejmowały wdrożenie systemów sieci aktywnych LAN/WiFi oraz ważny certyfikat potwierdzający wiedzę i umiejętności we wdrażaniu systemów zaoferowanych przez Wykonawcę, wystawiony przez producenta systemu lub dystrybutora lub autoryzowany ośrodek certyfikujący.

Zamawiający dopuszcza możliwość łączenia powyższych funkcji Specjalistów
w ramach jednej osoby. Wykonawca zobowiązany jest w takiej sytuacji wykazać, że wskazana osoba łącznie spełnia warunki, które Zamawiający określił dla poszczególnych Specjalistów w zakresie doświadczenia i posiadanych certyfikatów. W takim przypadku Zamawiający dopuszcza wykazanie spełnienia warunków w ramach tej samej umowy.

 Przed przystąpieniem do prac Wykonawca opracuje dokumentację zawierającą:

- schematy instalacyjne, elektryczne i logiczne,

- opis parametrów technicznych przyjętych rozwiązań technicznych,

- wykaz ilościowy wszystkich projektowanych materiałów,

- karty katalogowe projektowanych materiałów i urządzeń,

 Dokumentacja projektowa podlegać będzie najpierw akceptacji przez zarządców nieruchomości, a następnie zatwierdzeniu przez Zamawiającego. Wykonawca nie może przystąpić do realizacji zadania przed akceptacją dokumentacji przez Zamawiającego. Wszelkie zmiany w dokumentacji projektowej po jej zatwierdzeniu muszą być uzgodnione
z Zamawiającym.

 W trakcie realizacji robót Wykonawca jest zobowiązany do:

-zabezpieczenie i utrzymania w należytym porządku terenu robót,

-bezzwłocznej naprawy przypadkowych uszkodzeń instalacji,

-przygotowania i doprowadzenia do stanu pierwotnego terenu robót (w tym przestawienie mebli i urządzeń),

-występowania do Zamawiającego o zatwierdzenie planowanych do wbudowania materiałów przed ich zakupem,

-usuwania z terenu budowy materiałów nieodpowiadające wymaganiom,

-zgłaszania do odbioru przez Zamawiającego robót ulegających zakryciu,

-odpowiedniego zabezpieczenia składowanych materiałów,

- uporządkowania miejsca prowadzonych prac codziennie po zakończeniu prac.

 Utrudnienia mogące wystąpić w trakcie realizacji prac:

- obiekty mogą być czynne i wymagać bezwzględnej ciszy w określonych porach dnia (może być wymagana praca zmianowa),

- w obiektach mogą przebywać dzieci,

 - mogą wystąpić czasowe niedostępności pomieszczeń, wtedy należy z 3 dniowymi wyprzedzeniem poinformować zarządcę obiektu o planowanych pracach z podaniem przedziału czasowego niezbędnego do wykonania robót,

 - ograniczenia i obostrzenia wynikające z konieczności ograniczenia hałasu lub zapewnienia odpowiednich warunków sanitarno-epidemiologicznych,

 - prace na wysokości.

 Wykonawca wraz ze zgłoszeniem gotowości do odbioru przedłoży Zamawiającemu dokumentację powykonawczą, która musi zawierać opis stanu faktycznego i zawierać:

- dokumentację projektową wraz z naniesionymi zmianami,

- dokumenty potwierdzające prawidłowość zastosowanych materiałów (karty katalogowe, certyfikaty, deklaracje zgodności itd.