Załącznik 1 do Zapytania Ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia

w trybie zapytania ofertowego pn.:

Dostawa infrastruktury IT dla Trade & Travel Company

realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020

Łódź, czerwiec 2021 roku

Spis treści

ROZDZIAŁ 1 - PODSTAWOWE INFORMACJE 3

1.1. PRZEDMIOT ZAMÓWIENIA 3

1.2. TERMIN REALIZACJI 3

1.3. WYMAGANIA FORMALNE I ORGANIZACYJNE 3

1.4. WYMAGANIA OGÓLNE 4

1.5. SPOSÓB OBLICZENIA CENY OFERTY 5

1.6. ZASADY ODBIORU PRAC 5

1.7. UWARUNKOWANIA PRAWNE 5

ROZDZIAŁ 2 – SZCZEGÓŁOWY ZAKRES PRAC 6

2.1. Zabezpieczenie styku z Internetem – 1 sztuka 7

2.2. UPS – 1 sztuka ..... Błąd! Nie zdefiniowano zakładki.

2.3. Przełączniki dostępowe – 2 sztuki 10

2.4. Acess Pointy – 5 sztuk ..... Błąd! Nie zdefiniowano zakładki.

2.5. Serwery – 4 sztuki ..... Błąd! Nie zdefiniowano zakładki.

2.6. Macierz – 1 sztuka ..... Błąd! Nie zdefiniowano zakładki.

2.7. NAS – 1 sztuka 16

2.8. Komputery PC – 26 sztuk ..... Błąd! Nie zdefiniowano zakładki.

2.9. Laptopy – 4 sztuki ..... Błąd! Nie zdefiniowano zakładki.

2.10. Urządzenie wielofunkcyjne A3 – 1 sztuka ..... Błąd! Nie zdefiniowano zakładki.

2.11. Serwerowe systemy operacyjne – 4 sztuki ..... Błąd! Nie zdefiniowano zakładki.

2.12. Systemy operacyjne PC – 30 sztuk ..... Błąd! Nie zdefiniowano zakładki.

2.13. Pakiet biurowy – 30 sztuk ..... Błąd! Nie zdefiniowano zakładki.

ROZDZIAŁ 1 - PODSTAWOWE INFORMACJE

1.1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja sprzętu komputerowego oraz oprogramowania w biurach Zamawiającego. Zakres zamówienia jest następujący:

1.	Serwer domeny	szt. 1
2.	NAS	szt. 1
3.	System do backupu danych	szt. 1
4.	Komputery	szt. 9
5.	System operacyjny komputera	szt. 9
6.	Oprogramowania biurowe	szt. 9
7.	Przełączniki dostępowe	szt. 4
8.	Access Pointy	szt. 4
9.	UTM	szt. 2
10.	System operacyjny serwera	szt. 1
11.	System autoryzacji dostępu	szt. 30

1.2. TERMIN REALIZACJI

Zamawiający wymaga zrealizowania przedmiotu zamówienia w terminie 1 miesiąca od daty zawarcia umowy.

1.3. WYMAGANIA FORMALNE I ORGANIZACYJNE

1. Zamawiający wymaga wnikliwego zapoznania się z treścią OPZ.
2. OPZ stanowi podstawę opracowania oferty Wykonawcy, a po wyborze Wykonawcy, realizacji niniejszego zamówienia. Udzielanie wyjaśnień dotyczących zapisów zawartych w OPZ i ewentualne zmiany w ich treści są możliwe jedynie w toku postępowania ofertowego.
3. Wszelkie wątpliwości i zapytania ze strony Wykonawcy, powstałe w toku realizacji zadania, związane z zakresem, sposobem realizacji a także wystąpieniem sytuacji nieprzewidzianych w obowiązujących przepisach prawnych i w OPZ Wykonawca zobowiązany jest uzgadniać z Zamawiającym.
4. W ramach zamówienia przyjmuje się założenie neutralności technologicznej – nie wskazuje się i nie faworyzuje żadnej konkretnej technologii i oprogramowania (za wyjątkiem obowiązujących norm europejskich i krajowych oraz powszechnie stosowanych technologii o charakterze standardów),
5. W związku z obowiązkami Zamawiającego związanymi z realizacją projektu współfinansowanego ze środków UE, dotyczącymi działań informacyjnych i promocyjnych, na dokumentach związanych z realizowanym zadaniem, należy umieszczać znaki i oznaczenia zgodne z Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności., w tym:
   5.1. znak Unii Europejskiej wraz ze słownym odniesieniem do Unii Europejskiej;
   5.2. odniesienie do Funduszu;
   5.3. znak Fundusze Europejskie wraz z nazwą Program Regionalny.
6. Wzory znaków są dostępne na stronie http://www.rpo.lodzkie.pl.
7. Wykonawca zobowiązany jest do wyznaczenia Kierownika prac oraz osób, które upoważnione będą do kontaktów w sprawie realizacji zadania z Zamawiającym.
8. Wykonawca, na każdym etapie realizacji prac, zapewni stały i nieograniczony dostęp do wszelkich materiałów i dokumentów, które powstają w trakcie realizacji zadania Ponadto Wykonawca zobowiązuje się do stosowania zaleceń wydawanych przez Zamawiającego.

1.4. WYMAGANIA OGÓLNE

1. Zamawiający wymaga, aby system informatyczny powstały w wyniku realizacji niniejszego zamówienia funkcjonował zgodnie z obowiązującymi przepisami prawa oraz standardami technicznymi.
2. Zamawiający wymaga, aby dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej minimum na dzień poprzedzający dzień składania ofert.
3. Zamawiający wymaga, aby Wykonawca udzielił Zamawiającemu Licencji na użytkowanie dostarczonego oprogramowania.
4. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
5. Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (nie były używane).
6. Wszystkie dostarczane urządzenia, sprzęt i oprogramowanie muszą pochodzić z autoryzowanego w UE kanału sprzedaży producenta zaoferowanych urządzeń i oprogramowania.
7. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji.
8. Zamawiający wymaga, aby dostarczony urządzenia był zasilany prądem przemiennym o napięciu 230V z tolerancją +/- 5% i częstotliwości wejściowej 50-60 Hz.
9. Zamawiający zastrzega sobie prawo do sprawdzenia zgodności funkcjonalnej, technicznej oraz legalności dostaw bezpośrednio u polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych
10. W wypadku powzięcia wątpliwości, co do zgodności z Umową, w szczególności w zakresie legalności Oprogramowania, Zamawiający jest uprawniony do:
    10.1. zwrócenia się do producenta o potwierdzenie ich zgodności z Umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz
    10.2. zlecenia producentowi lub wskazanemu przez producenta podmiotowi, inspekcji pod kątem zgodności z Umową oraz ważności i zakresu uprawnień licencyjnych.
11. Jeżeli inspekcja, o której mowa powyżej wykaże niezgodność z Umową lub stwierdzi, że korzystanie z Oprogramowania narusza majątkowe prawa autorskie producenta lub osób trzecich, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 30% wartości Przedmiotu Umowy (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w wyniku dokonanej inspekcji, jak np. konieczność zakupu nowego oprogramowania, czy też roszczeń odszkodowawczych osób trzecich). Prawo zlecenia inspekcji nie ogranicza, ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia Oprogramowania zgodnych z Umową oraz roszczeń odszkodowawczych.
12. Wykonawca jest odpowiedzialny za wszelkie wady fizyczne w wykonanych pracach.
13. Wykonawca jest odpowiedzialny za wszelkie wady prawne, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem ich do obrotu na terytorium Rzeczypospolitej Polskiej.
14. Wykonawca odpowiada za wszelkie naruszenia praw osób trzecich, które mogą wystąpić w związku z wykonywaniem przedmiotu zamówienia.
15. Wykonawca odpowiada za wszelkie szkody związane z realizacją przedmiotu zamówienia wynikające z przyczyn leżących po stronie Wykonawcy lub podmiotów, którymi przy wykonywaniu zamówienia będzie się posługiwał.
16. Zamawiający informuje, że jeżeli w ZO zostały wskazane typy i symbole materiałów lub urządzeń oraz nazwy ich producentów to mają one jedynie charakter przykładowy. Zostały określone jedynie w celu sprecyzowania parametrów i wymogów techniczno-użytkowych przedmiotu zamówienia.
17. Zamawiający dopuszcza zastosowanie rozwiązań równoważnych. Powołując się na rozwiązania równoważne w stosunku do opisywanych przez Zamawiającego, Wykonawca jest obowiązany wykazać, że oferowane przez niego rozwiązanie równoważne będzie posiadać funkcjonalność zgodną z posiadaną i wymaganą przez Zamawiającego.
18. Niewykazanie równoważności zaoferowanych urządzeń traktowane będzie, jako deklaracja zastosowania rozwiązania wymienionego w ZO.

1.5. SPOSÓB OBLICZENIA CENY OFERTY

W cenie oferty Wykonawca winien skalkulować wszelkie koszty jakie poniesie w związku z realizacją zamówienia, w tym w szczególności: czasu pracy, wykorzystanych materiałów i urządzeń, czynności konserwacyjnych, ubezpieczenia, magazynowania, transportu, rozładunku, wymaganego oznaczenia, dokonania odbiorów, gwarancji, kosztów licencji, koszty instalacji, konfiguracji, wdrożenia oprogramowania, migracji danych, o ile taka migracja danych (zależna od zakresu i przedmiotu oferty Wykonawcy) będzie konieczna dla prawidłowej realizacji zamówienia oraz koszty wymaganych prawem opłat i podatków, a także wszystkie inne dodatkowe koszty, które powstaną w trakcie realizacji zamówienia.

1.6. ZASADY ODBIORU PRAC

1. Wykonawca zgłosi przedmiot zamówienia do kontroli Zamawiającego.
2. Zgłoszenie do odbioru może nastąpić po przedstawieniu Zamawiającemu Dokumentacja Powykonawcza
3. Dokumentacja Powykonawcza przedmiotu zamówienia musi zawierać:
   - 3.1. Informacje podstawowe o projekcie
   - 3.2. Wykaz dostarczonego sprzętu, oprogramowania i urządzeń wraz z :
     - 3.2.1. numerami produktów
     - 3.2.2. numerami licencji,
     - 3.2.3. wykonawcą oraz okresem gwarancji i opieki aktualizacyjnej
   - 3.3. Architekturę wykonanego środowiska
   - 3.4. Opis podstawowych procedur administracyjnych
   - 3.5. Zamawiający wymaga by Dokumentacja Powykonawcza została dostarczona Zamawiającemu w postaci dokumentu sporządzonego w języku polskim w liczbie 2 egzemplarzy w formie papierowej oraz w wersji elektronicznej na nośniku, w formie plików edytowalnych (np. typu: docx, xlsx, pdf, vsdx).
4. Zamawiający w terminie do 5 dni roboczych wykona kontrolą zgłoszonego przedmiotu zamówienia, w zakresie zgodności wykonania przedmiotu prac z OPZ, technologią;
5. W przypadku pozytywnego wyniku kontroli, Zamawiający odbierze przedmiot zamówienia i podpisze Protokół Odbioru Końcowego.
6. W przypadku stwierdzenia niezgodności z OPZ i/lub usterek Wykonawca zobowiązany jest do ich usunięcia w terminie do 5 dni roboczych od dnia otrzymania od Zamawiającego informacji o stwierdzonych zastrzeżeniach do przedmiot zamówienia.
7. Naruszenie terminu wynikającego z przekroczenia terminu usunięcia usterek stwierdzonych w trakcie kontroli, stanowić będzie podstawę do naliczenia kar umownych za nieterminową realizację umowy.
8. Umowę będzie uważać się za wykonaną w terminie, pod warunkiem, podpisania przez Zamawiającego Protokół Odbioru Końcowego przed terminem określonym w punkcie 1.2.
9. Zamawiający może odmówić odbioru przedmiotu zamówienia w przypadku, gdy nie został on wykonany w sposób określony w OPZ, zgodnie z zasadami sztuki i wiedzy zawodowej lub przepisami prawa.

1.7. UWARUNKOWANIA PRAWNE

Wykaz aktów prawnych określających uwarunkowania prawne realizacji przedmiotu zamówienia:

1. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000);
2. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz. U. z 2016 r., poz. 113).
3. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”

ROZDZIAŁ 2 –SZCZEGÓŁOWY ZAKRES PRAC

1. Elementem realizacji zamówienia jest dostawa sprzętu, urządzeń oraz licencji oprogramowania oraz ich instalacja, konfiguracja oraz produkcyjne uruchomienie.
2. Sprzęt, urządzenia i oprogramowania zgodne z wymaganiami określonymi w niniejszym rozdziale muszą zostać dostarczone do siedziby Zamawiającego wraz z niezbędnym do użytkowania osprzętem i przewodami zasilającymi i podłączeniowymi.
3. Szczegółową informację o docelowych pomieszczeniach, w których powinien być rozmieszczony i zainstalowany sprzęt, Wykonawca otrzyma w terminie do 5 dni od daty podpisania umowy na wykonanie niniejszego zamienienia.
4. Warunkiem konieczny przystąpienia do instalacji i konfiguracji urządzeń i oprogramowania jest zaakceptowany przez Zamawiającego Harmonogram prac instalacyjnych i konfiguracyjnych.
5. W przypadku braku zaakceptowanego Harmonogramu prac Wykonawcy nie zostanie udzielony dostęp do pomieszczeń i środowiska informatycznego Zamawiającego, z winy Wykonawcy.
6. Wykonawca ponosi odpowiedzialność za wszelkie szkody wyrządzone Zamawiającemu, innym użytkownikom lub osobom trzecim w związku z realizacją zamówienia.
7. Wykonawca zobowiązany jest do przestrzegania obowiązujących przepisów i instrukcji obowiązujących w miejscu instalacji. Wykonawca zobowiązany jest do zapoznania się z odpowiednimi przepisami i instrukcjami.
8. Podczas prac instalacyjnych Wykonawca musi zachować następującą kolejność prac:
   8.1. powiadomić Zamawiającego na minimum 5 dni przed rozpoczęciem prac instalacyjnych
   8.2. zainstalować i skonfigurować dostarczony sprzęt, urządzenia i oprogramowanie
   8.3. dokonać weryfikacji poprawności działania.
9. Przedmiot zamówienia należy dostarczyć, zainstalować i skonfigurować w biurach Zamawiającego:
   9.1. w Łodzi przy ul. Piotrkowska 92;
   9.2. w Warszawie przy ulicy Koszykowej 53.

2.1. Serwer domeny

Do obowiązków Wykonawcy należy dostawa do Zamawiającego serwera domeny, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

Wymagane minimalne parametry techniczne:

Lp.	Parametr	Minimalne wymagania
1	Zastosowanie	Wykorzystywany dla potrzeb aplikacji medycznych, biurowych, dostępu do zasobów lokalnej sieci komputerowej oraz usług sieci Internet, a także danych multimedialnych.
2	Procesor	Procesor klasy x86 ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych, zapewniający wydajność min. 9000 pkt. w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php
3	Płyta główna	– chipset dostosowany do oferowanego procesora lub równoważny – minimum 2 sloty pamięci , obsługującej częstotliwość minimum 2666 MHz lub więcej – minimum 1 x PCI Express 3.0 x 16 – minimum 1 x PCI Express 2.0 x 1 – minimum 2 złącza SATA 6.0 Gb/s
4	Pamięć operacyjna RAM	– minimum 16 GB DDR4 – minimum 1 wolny slot pamięci na płycie głównej, – minimalny rozmiar możliwego rozszerzenia obsługiwanej pamięci: 64 GB
5	Porty	– minimum 1 x Display Port, – minimum 4 x USB, w tym minimum 2x USB 3.0 – minimum 1 x DVI lub 1 x HDMI – minimum 1 port sieciowy RJ-45, – porty słuchawek i mikrofonu lub port combo Wymagana ilość portów USB, oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
6	Dysk twardy	Minimum 500 GB SSD NVMe, samoszyfrujący, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego zainstalowanego na komputerze przez producenta, po awarii, do stanu fabrycznego (tryb OOBE dla systemu MS Windows)
7	Karta dźwiękowa	Karta dźwiękowa zintegrowana z płytą główną, zgodna ze standardem High Definition
8	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.0, OpenCL 1.2
9	Karta sieciowa	10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną, wspierająca obsługę technologii WoL
10	BIOS	BIOS UEFI w wersji 2.6 lub wyższej. Możliwość odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym, - AssetTag/IDTag - MAC Adres karty sieciowej, - wersja Biosu wraz z datą jego produkcji, - zainstalowanym procesorze, jego taktowaniu - ilości pamięci RAM wraz z taktowaniem i obłożeniem slotów Możliwość z poziomu BIOS: - wyłączenia selektywnego portów USB, minimum wyłączanie portów z przodu oraz wyłączanie portów z tyłu jako grup - wyłączenia selektywnego (pojedynczego) portów SATA, - zmiany pracy wentylatorów między trybem optymalizacji głośności lub temperatury, - ustawienia hasła: administratora, Power-On, HDD, - możliwość zbierania i przeglądania logów zdarzeń z informacją odnośnie godziny, daty i kodu błędu zdarzenia - ustawienie automatycznej aktualizacji BIOS z serwera producenta komputera
11	Klawiatura	Klawiatura USB w układzie polskim programisty (105 klawiszy) z kablem o długości min. 1,8 m.
12	Mysz	Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m.

13	Obudowa	Typu Tower, MT lub rack z możliwością pracy w pozycji pionowej i poziomej (dostarczony komplet nóżek dla obu orientacji), z obsługą kart PCI Express wyłącznie o niskim profilu. Wbudowany głośnik.
14	Zasilanie	Zasilacz o mocy nie większej niż 280 W o sprawności co najmniej 92% przy obciążeniu 50%. Roczny pobór mocy, nie większy, niż w specyfikacji energetycznej dla Energy Star w wersji 7.1
15	Bezpieczeństwo i funkcje zarządzania	Moduł TPM 2.0; Oprogramowanie zaimplementowane w BIOS umożliwiające – bez względu na stan czy obecność systemu operacyjnego oraz bez podłączania żadnych urządzeń czy nośników zewnętrznych - w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego. Usuwanie danych z dysku twardego musi odbywać się przy wykorzystaniu certyfikowanych algorytmów a wynikiem pracy oprogramowania musi być protokół zawierający dane kasowanego dysku oraz informacje o zastosowanym algorytmie kasowania. W ofercie należy podać nazwę i producenta oprogramowania. System diagnostyczny działający bez udziału systemu operacyjnego, czy też jakichkolwiek dołączonych urządzeń na zewnątrz czy też wewnątrz komputera, umożliwiający otrzymanie informacji o: modelu, oznaczeniu i numerze seryjnym komputera, pojemności zainstalowanej pamięci RAM; Oprogramowanie diagnostyczne musi umożliwiać: - wykonanie testu pamięci RAM, - wykonanie podstawowego testu prawidłowej pracy CPU - wykonanie testu dysku twardego. System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera (Zaimplementowany w sprzętowym mikrokodzie płyty głównej)
16	Sterowniki i oprogramowanie	Zapewnienie na dedykowanej stronie internetowej producenta dostępu do najnowszych sterowników i uaktualnień, realizowane poprzez podanie numeru seryjnego/modelu urządzenia, podać link strony www. Oprogramowanie producenta komputera posiadające funkcje zarządzania sterownikami (wykrywanie oraz instalowanie aktualizacji). Oprogramowanie pozwalające z poziomu BIOS-u komputera wykonać automatyczną aktualizację BIOS z serwera producenta komputera bądź serwera klienta.
17	Certyfikaty i oświadczenia	1. Producent komputera musi posiadać ISO 9001 co najmniej w zakresie projektowania, produkcji i serwisu komputerów. 2. Producent komputera musi posiadać ISO 14001, co najmniej w zakresie projektowania i produkcji. 3. Oferowane komputery stacjonarne muszą posiadać europejską deklarację zgodności CE. 4. Producent komputera musi posiadać normę ISO 27001. 5. Certyfikat TCO – obecność modelu na stronie https://tcocertified.com/product-finder/ 6. Certyfikat EPEAT dla standardu IEEE 1680.1 - 2018 – obecność modelu na stronie https://www.epeat.net/?category=pcsdisplays
18	Zainstalowane oprogramowanie systemowe	Zgodne z wymaganiami określonymi w rozdziale 2.10

.

2.2. NAS

Do obowiązków Wykonawcy należy dostawa do Zamawiającego jednego serwera NAS, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.
Wymagane minimalne parametry techniczne:

1. Obudowa wolnostojąca lub typu rack
2. Wskaźniki LED: LAN, HDD, Status,
3. Cztery zatoki na dyski 2,5”/3,5’ ’HDD SATA , hot swap. 6 Gb/s lub SSD
4. Procesor czterordzeniowy w architekturze 64 bitowej z zegarem o częstotliwości min. 2,0 GHz
5. Pamięć RAM systemowa 4 GB DDR4
6. Zainstalowane dyski: 4 dyski:
   6.1. HDD SATA III, 6 Gb/s,
   6.2. w technologii hot-swap
   6.3. pojemność każdego dysku 8 TB,
   6.4. cache 256 MB
   6.5. prędkość obrotowa 5400 obr/min
7. Oprogramowanie zarządzające z możliwością szyfrowania dysków, wolumenów
8. Wbudowane karty sieciowe: 2 porty RJ-45 GigabitEthernet
9. Wbudowane porty USB: 4 porty USB , w tym min 2 portu USB 3.0 (USB 3.1 gen1)
10. Dostępna konfiguracja RAID 0, 1, 5, 6, 10
11. System plików - EXT4

2.3. System do backupu danych

Do obowiązków Wykonawcy należy dostawa do Zamawiającego system do backupu danych, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.
Wymagane minimalne parametry techniczne:

1. Obudowa wolnostojąca lub typu rack
2. Wskaźniki LED: LAN, HDD, Status,
3. Cztery zatoki na dyski 2,5”/3,5’ ’HDD SATA , hot swap. 6 Gb/s lub SSD
4. Procesor czterordzeniowy w architekturze 64 bitowej z zegarem o częstotliwości min. 2,0 GHz
5. Pamięć RAM systemowa 4 GB DDR4
6. Zainstalowane dyski: 4 dyski:
   6.1. HDD SATA III, 6 Gb/s,
   6.2. w technologii hot-swap
   6.3. pojemność każdego dysku 8 TB,
   6.4. cache 256 MB
   6.5. prędkość obrotowa 5400 obr/min
7. Oprogramowanie zarządzające z możliwością szyfrowania dysków, wolumenów
8. Wbudowane karty sieciowe: 2 porty RJ-45 GigabitEthernet
9. Wbudowane porty USB: 4 porty USB , w tym min 2 portu USB 3.0 (USB 3.1 gen1)
10. Dostępna konfiguracja RAID 0, 1, 5, 6, 10
11. System plików - EXT4

2.4. Komputery

Do obowiązków Wykonawcy należy dostawa do Zamawiającego **9 sztuk** komputerów przenośnych, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja.

Wymagane minimalne parametry techniczne:

Lp.	Parametr	Minimalne wymagania
1	Zastosowanie	Notebook będzie wykorzystywany dla potrzeb aplikacji medycznych, finansowych, biurowych, aplikacji graficznych, dostępu do Internetu oraz poczty elektronicznej.
2	Ekran	Dotykowy umożliwiający wybieranie, przesuwanie i klikanie wszystkich elementów na ekranie Przekątna minimum 15" z tolerancją -1”/ +0,6” Rozdzielczość : FHD+ 1920 x 1080 pixeli Matryca IPS z podświetlaniem LED. Jasność minimum300 nitów. Kontrast minimum 1000:1. Kąt widzenia minimum 170 stopni
3	Procesor	Procesor: osiągający w teście PassMark Performance Test, wynik CPU Mark, na podstawie wyników ze strony www.cpubenchmark.net – wynik nie mniejszy niż 6.000 punktów
4	Pamięć RAM	Pamięć RAM: 8GB DDR3 z możliwością rozbudowy do 16GB.
5	Dysk	250 GB SSD
6	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki.
7	Touchpad	Touchpad wyposażony w 2 niezależne klawisze funkcyjne ze wsparciem dla technologii multitouch. Musi posiadać wsparcie dla gestów dla minimum 3 niezależnych punktów dotyku.
8	Klawiatura	Klawiatura, pełnowymiarowa podświetlana klawiatura typu chiclet; skok 1,3 mm +/- 0,15 mm
9	Multimedia	karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o mocy 2W. mikrofon z funkcja redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. kamera internetowa HD (720p) zainstalowana w obudowie wraz z diodą LED.
10	Obudowa	Obudowa: zawias obracany o 360 stopni, który umożliwia pracę w czterech trybach — tabletu, namiotu, laptopa i podstawki.
11	Głośnik	Głośnik
12	Porty , gniazda:	Gniazdo na kartę Micro SD 2xUSB 3.x 1 x USB 2.x Złącze HDMI Gniazdo słuchawkowe Moduł Bluetooth 4.1. Zintegrowana karta sieci WLAN, obsługująca łącznie standardy IEEE 802.11 a/b/g/n/ac
13	Bateria	Bateria: minimum 3-komorowa, 40 Wh
14	Zasilacz	Zasilacz
15	Waga	Waga: maksymalnie 1,75 kg z baterią.
16	Mysz	Mysz optyczna, bezprzewodowa

2.5. System operacyjny komputera

Do każdego z komputerów opisanych w rozdziale 2.4 powyżej musi być dostarczone oprogramowanie systemu operacyjnego spełniającego minimum następujące funkcjonalności:
Najnowszy stabilny system operacyjny, przeznaczony dla architektury 64 bitowej, spełniający następujące wymagania poprzez wbudowane mechanizmy (bez użycia dodatkowych aplikacji):

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   1.1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   1.2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,a
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługastandardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy logowania do domeny w oparciu o:

26.1. Login i hasło,
26.2. karty z certyfikatami (smartcard),
27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
28. Mechanizmy wieloelementowego uwierzytelniania.
29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
31. Wsparcie dla algorytmów Suite B (RFC 4869),
32. Wsparcie wbudowanej zapory ogniowej Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
33. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
34. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
35. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
36. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
37. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
38. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
39. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
40. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
41. Udostępnianie modemu,
42. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
43. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci
44. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
45. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
46. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
47. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
48. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
49. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
50. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

2.6. Oprogramowania biurowe

Do każdego z komputerów opisanych w rozdziale 2.4 musi być dostarczone oprogramowanie systemu biurowego spełniającego minimum następujące funkcjonalności:

1. Wymagania ogólne:
   - 1.1. Pełna polska wersja językowa interfejsu użytkownika
   - 1.2. Intuicyjność obsługi,
   - 1.3. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się
   - 1.4. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
     - 1.4.1. posiada kompletny i publicznie dostępny opis formatu,
     - 1.4.2. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
     - 1.4.3. umożliwia wykorzystanie schematów XML
     - 1.4.4. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   - 1.5. Oprogramowanie musi umożliwiać dostosowanie dokumentów do potrzeb oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców
   - 1.6. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy)
   - 1.7. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim
   - 1.8. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
     - 1.8.1. edytor tekstu
     - 1.8.2. arkusz kalkulacyjny
     - 1.8.3. narzędzie do przygotowywania i prowadzenia prezentacji
   - 1.9. narzędzie do zarządzania informacją (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)"
   - 1.10. Wymagania zawarte w specyfikacjach poszczególnych produktów odnoszą się do natywnej funkcjonalności oferowanego oprogramowania bez użycia dodatkowego oprogramowania.
   - 1.11. Licencja musi uwzględniać prawo (w okresie przynajmniej 3 lat) do bezpłatnej instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych
   - 1.12. Zamawiający wymaga dostarczenia kompletu wymaganych kluczy aktywacyjnych.
   - 1.13. Zamawiający wymaga dostarczenia dokumentów pozwalających na stwierdzenie legalności zakupionego oprogramowania dla celów inwentaryzacyjnych i audytowych
   - 1.14. Telefoniczne wsparcie techniczne w języku polskim.
2. Edytor tekstu musi umożliwiać:
   - 2.1. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   - 2.2. Wstawianie oraz formatowanie tabel
   - 2.3. Wstawianie oraz formatowanie obiektów graficznych
   - 2.4. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
   - 2.5. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
   - 2.6. Automatyczne tworzenie spisów treści
   - 2.7. Formatowanie nagłówków i stopek stron
   - 2.8. Sprawdzanie pisowni w języku polskim
   - 2.9. Śledzenie zmian wprowadzonych przez użytkowników
   - 2.10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   - 2.11. Określenie układu strony (pionowa/pozioma)
   - 2.12. Wydruk dokumentów

2.13. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
2.14. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, Microsoft Word 2007 lub Microsoft Word 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
2.15. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
2.16. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
2.17. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

3. Arkusz kalkulacyjny musi umożliwiać
3.1. Tworzenie raportów tabelarycznych
3.2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
3.3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu
3.4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
3.5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
3.6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
3.7. Wyszukiwanie i zmianę danych
3.8. Wykonywanie analiz danych przy użyciu formatowania warunkowego
3.9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
3.10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
3.11. Formatowanie czasu, daty i wartości finansowych z polskim formatem
3.12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku
3.13. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, Microsoft Excel 2007oraz Microsoft Excel 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń
3.14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

4. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać
4.1. Prezentowanie przy użyciu projektora multimedialnego
4.2. Drukowanie w formacie umożliwiającym robienie notatek
4.3. Zapisanie, jako prezentacji tylko do odczytu
4.4. Nagrywanie narracji i dołączanie jej do prezentacji
4.5. Opatrywanie slajdów notatkami dla prezentera
4.6. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
4.7. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
4.8. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
4.9. Możliwość tworzenia animacji obiektów i całych slajdów
4.10. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
4.11. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i MS PowerPoint 2010

4.12. Możliwość publikacji prezentacji i jej prowadzenie z zewnętrznego źródła internetowego umożliwiającego oglądanie prezentacji przez użytkowników zewnętrznych posługujących się przeglądarką.

5. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
   5.1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
   5.2. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
   5.3. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
   5.4. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
   5.5. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
   5.6. Zarządzanie kalendarzem
   5.7. Udostępnianie kalendarza innym użytkownikom
   5.8. Przeglądanie kalendarza innych użytkowników
   5.9. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
   5.10. Zarządzanie listą zadań
   5.11. Zlecanie zadań innym użytkownikom
   5.12. Zarządzanie listą kontaktów
   5.13. Udostępnianie listy kontaktów innym użytkownikom
   5.14. Przeglądanie listy kontaktów innych użytkowników
   5.15. Możliwość przesyłania kontaktów innym użytkowników.

2.7. Przełączniki dostępowe

Do obowiązków Wykonawcy należy dostawa do Zamawiającego 4 przełączników dostępowych, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja i konfiguracja.
Dopuszcza się, aby elementy wchodzące w skład opisanego poniżej urządzenia były zrealizowane w postaci jednej zamkniętej platformy sprzętowej lub w postaci kilku osobnych urządzeń realizujących opisane poniżej wymagania techniczne lub też były częścią większego zestawu funkcjonalnego zrealizowanego jako jedno urządzenie.

Wymagane minimalne parametry techniczne:

L.p.	Nazwa parametru
	Typ i liczba portów: a) Minimum 12 portów gigabitowych w standardzie 100/1000BaseT, b) Minimum 1 port Gigabit SFP
2.	Zasilanie poprzez PoE innych urządzeń możliwe na wszystkich portach Ethernet zgodnie ze standardem PoE+ 802.3af/at lub pasywnym PoE 24 V
3.	Domyślne wykrywanie urządzenia 802.3af/at,
4.	Moc na port - 34,2 W dla PoE+ lub 17 W dla pasywnego PoE
5.	Całkowita moc maksymalna: 250 W na wszystkie porty
6.	Routing IPv4 – minimum: statyczny, RIPv2, OSPF
7.	Routing IPv6 – minimum: statyczny, RIPng, OSPFv3
8.	Wielkość sprzętowej tablicy rutingu: a) minimum 1000 wpisów dla IPv4, b) minimum 500 wpisów dla IPv6.
9.	Obsługa ruchu Multicast: a) IGMP Snooping, b) MLD Snooping.
10.	Obsługa vlan.
11.	Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.
12.	Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN
13.	Przepustowość non-blocking 26 Gb/s
14.	Przepustowość przełączania 52 Gb/s
15.	Prędkość przekazywania 38,69 Mpps
16.	Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping.
17.	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.
18.	Obsługa standardu 802.1p
19.	Funkcja mirroringu portów.
20.	Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az.
21.	Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
22.	Obsługa Syslog.
23.	Obsługa SNTPv4.
24.	Certyfikaty: CE / FCC / IC; ETSI300-019-1.4
25.	Minimalny zakres pracy od -5°C do 40°C.
26.	Wewnętrzny zasilacz 230V.

2.8. Access Point

Do obowiązków Wykonawcy należy dostawa do Zamawiającego 4 punktów dostępu do sieci WiFi, spełniającego min. wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja i konfiguracja.
Dopuszcza się, aby elementy wchodzące w skład opisanego poniżej urządzenia były zrealizowane w postaci jednej platformy sprzętowej lub też były częścią większego zestawu funkcjonalnego zrealizowanego jako jedno urządzenie.
Wymagane minimalne parametry techniczne:

Lp.	Parametr	Minimalne wymagania
1	Interfejs sieciowy	1 gigabitowy port Ethernet
2	Sposób zasilania	PoE 802.3af
3	Maksymalny pobór mocy	10,5 W
4	Zakres napięcia wejściowego	44 - 57 V DC
5	Moc nadawcza	2,4 GHz: 23 dBm
		5 GHz: 26 dBm
6	MIMO	2,4 GHz: 2x2
		5 GHz: 4x4
7	Maks. teoretyczna przepustowość	2,4 GHz: 300 Mb/s
		5 GHz: 1733 Mb/s
8	Anteny	2,4 GHz: 2 dookólne anteny o zysku 2,8 dBi
		5 GHz: 2 dookólne anteny (podwójna polaryzacja) 3 dBi
9	Standardy WiFi	802.11 b/g/n
		802.11 a/n/ac/ac-wave2
		802.11 r/k/v
10	Zabezpieczenia	WEP
		WPA-PSK
		WPA-Enterprise (WPA/WPA2, TKIP/AES)
		802.11w/PMF
11	BSSID	4 na radio
12	Montaż	Na ścianie lub suficie (uchwyt w zestawie)
13	Dopuszczalna temperatura pracy	Od -10 do 70 st. C
14	Dopuszczalna wilgotność powietrza	5%-95% niekondensująca
15	Certyfikaty	CE, FCC, IC
16	VLAN	802.1Q
17	QoS	Limit na użytkownika
18	Izolacja ruchu gości	Tak
19	WMM	Voice, video, best effort, background
20	Maks. ilość podłączonych użytkowników	200+
21	802.11b	1, 2, 5.5, 11 Mb/s
22	802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mb/s
23	802.11n	6,5 - 300 Mb/s
		MCS0 - MCS15
		HT 20/40
24	802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mb/s
25	802.11ac	6,5 Mb/s - 1,7 Gb/s
		MCS0 - MCS9 NSS1/2/3/4
		VHT 20/40/80
		54 Mb/s - 1,7 Gb/s
		MCS0 - MCS9 NSS1/2

2.9. UTM

Do obowiązków Wykonawcy należy dostawa do Zamawiającego dwóch urządzeń zabezpieczających styk z Internetem – UTM-ów, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja. Dopuszcza się, aby elementy wchodzące w skład zabezpieczenie styku z Internetem były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci kilku osobnych urządzeń realizujących opisane poniżej wymagania techniczne lub też były częścią większego zestawu funkcjonalnego zrealizowanego jako jedno urządzenie lub też w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Wymagane minimalne parametry techniczne:

1. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów:
   1.1. router/NAT
   1.2. transparent.
2. Porty:
   2.1. 2 interfejsy miedziane Ethernet 10/100/1000 Mb/s
   2.2. 2 porty Combo RJ45/SFP 10/100/1000 Mb/s
3. Wydajność przekazywania pakietów (Layer 3):
   3.1. Pakiety 64 bajtowe: 2.400.000 pps
   3.2. Pakiety 512 bajtowe: 4 Gbps
4. Pamięć RAM 2 GB DDR3
5. Pamięć wbudowana 4 GB pamięci Flash
6. Możliwość tworzenia interfejsów wirtualnych definiowanych jako VLAN w oparciu o standard 802.1Q.
7. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
8. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności systemu bezpieczeństwa, mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
   8.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
   8.2. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
   8.3. Poufność danych - IPSec VPN oraz SSL VPN
   8.4. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
   8.5. Kontrola stron Internetowych – Web Filter [WF]
   8.6. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)
   8.7. Kontrola pasma oraz ruchu [QoS i Traffic shaping]
   8.8. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
   8.9. Analiza ruchu szyfrowanego protokołem SSL
9. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
   9.1. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
   9.2. klient VPN współpracującego z proponowanym rozwiązaniem
   9.3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
   9.4. Praca w topologii Hub and Spoke oraz Mesh
   9.5. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth
   9.6. Obsługa ssl vpn w trybach portal oraz tunel

10. Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
11. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
12. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
13. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
14. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
15. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących ochronę przed atakami typu DoS oraz DDos.
16. Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
17. Baza filtra WWW. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
18. Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
19. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
20. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe,
21. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą min:
    21.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    21.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    21.3. Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
22. System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
23. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ dla rozwiązań kategorii Network Firewall.
24. Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
25. Certyfikaty: CE, FCC, IC

2.10. System operacyjny serwera

Do serwera domeny opisanego w rozdziale 2.1 musi być dostarczone oprogramowanie systemu operacyjnego spełniającego minimum następujące funkcjonalności:
Najnowszy stabilny system operacyjny, przeznaczony dla architektury 64 bitowej, spełniający następujące wymagania poprzez wbudowane mechanizmy (bez użycia dodatkowych aplikacji):

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   1.1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   1.2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,a
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługastandardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy logowania do domeny w oparciu o:

26.1. Login i hasło,
26.2. karty z certyfikatami (smartcard),
27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
28. Mechanizmy wieloelementowego uwierzytelniania.
29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
31. Wsparcie dla algorytmów Suite B (RFC 4869),
32. Wsparcie wbudowanej zapory ogniowej Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
33. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
34. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
35. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
36. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
37. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
38. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
39. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
40. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
41. Udostępnianie modemu,
42. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
43. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci
44. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
45. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
46. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
47. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
48. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
49. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
50. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
51. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

2.11. System autoryzacji dostępu

W ramach niniejszego zamówienia Zamawiający wymaga wdrożenia dla minimum 30 pracowników Zamawiającego, systemu autoryzacji dostępu do zasobów informatycznych Zamawiającego, spełniającego minimum następujące funkcjonalności:

1. Zarządzanie aplikacjami w chmurze i lokalnymi przy użyciu serwera proxy aplikacji, logowania jednokrotnego i aplikacji typu oprogramowanie jako usługa (SaaS).
2. Zarządzanie samoobsługowym resetowaniem haseł, uwierzytelnianiem wieloskładnikowym, niestandardowymi listami zakazanych haseł i inteligentną blokadą usługi autoryzacji dostępu.
3. Zarządzanie użytkownikami-gośćmi i partnerami zewnętrznymi przy zachowaniu kontroli nad danymi firmowymi.
4. Dostosowywanie i kontrolowanie sposobu tworzenia kont, logowania się i zarządzania profilami przez użytkowników podczas korzystania z aplikacji.
5. Zarządzanie dostępem do aplikacji w chmurze.
6. Zarządzanie sposobem uzyskiwania dostępu do danych firmowych przez urządzenia w chmurze lub lokalne.
7. Przyłączanie maszyn wirtualnych do domeny bez używania kontrolerów domeny.
8. Zarządzanie przypisywaniem licencji i dostępem do aplikacji oraz konfigurowanie delegatów za pomocą grup i ról administratora.
9. Tożsamość hybrydowa - udostępnianie pojedynczej tożsamości użytkownika na potrzeby uwierzytelniania i autoryzacji we wszystkich zasobach, niezależnie od lokalizacji (w chmurze lub lokalnie).
10. Zarządzanie tożsamością w organizacji za pośrednictwem mechanizmów kontroli dostępu pracowników, partnerów biznesowych, dostawców, usług i aplikacji.
11. Etapy wdrożenia systemu autoryzacji dostępu
    - 11.1. Utworzenie domeny.
    - 11.2. Utworzenie schematu organizacyjnego.
    - 11.3. Utworzenie folderów udostępnionych.
    - 11.4. Nadanie uprawnień do folderów po wcześniejszym uzgodnieniu macierzy uprawnień.
    - 11.5. Konfiguracja polityki zabezpieczeń.
    - 11.6. Konfiguracja kopii bezpieczeństwa.
    - 11.7. Instalacja drukarek oraz uzrądzeń wielofunkcyjnych na serwerze oraz konfiguracja serwera wydruku.
    - 11.8. Instalacja WSUS.
    - 11.9. Podłączenie komputerów do utworzonej domeny.
    - 11.10. Migracja danych.
    - 11.11. Wdrożenie WSUS na komputerach.
    - 11.12. Instalacja odpowiednich drukarek/urządzeń wielofunkcyjnych na komputerach.
    - 11.13. Konfiguracja VPN.
    - 11.14. Dokumentowanie wykonanych prac.