# **Załącznik nr 7 SWZ – opis przedmiotu zamówienia dla części II**

**część II - dostawa i instalacja sprzętu komputerowego**

# Wstęp

W ramach zadania wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie”.

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

1. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
2. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane
3. Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
4. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
5. Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
6. Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
7. połączenie urządzeń będzie zrealizowane w sposób nieograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
8. łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
9. zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
10. wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
11. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;

## Torby do laptopa (4 szt.)

Zamawiający przewiduje 4 torby na laptopa o wymiarach min 15,6 cala, z paskiem na ramię i uchwytem.

## OPROGRAMOWANIE DO PROJEKTOWANIA GRAFICZNEGO (TWORZENIE ILUSTRACJI, UKŁADU STRON) (6 szt.)

Minimalne, wymagane parametry:

Oprogramowanie do projektowania graficznego (tworzenie ilustracji, układu stron) – licencja dożywotnia

Wszechstronne oprogramowanie do projektowania graficznego – licencja dostarczona w najnowszej wersji, nie może być to wersja edukacyjna

Oprogramowanie powinno posiadać następujące elementy oraz cechy:

* umożliwiać projektowani grafiki i układy stron, edytować zdjęcia oraz tworzyć witryny internetowe.
* mieć możliwości wyświetlania na kilku monitorach i korzystania z wyświetlaczy o rozdzielczości 4K
* pozwalać użytkownikom na proste i szybkie uzyskiwanie profesjonalnych rezultatów.
* wbudowane narzędzia powinny być intuicyjne oraz posiadać możliwość tworzenia logotypów, broszur, grafik internetowych, reklam do serwisów społecznościowych, billboardy i innych oryginalnych projektów
* powinno posiadać przewodnik startowy mieć możliwość tworzenia obszaru roboczego dostosowanego do własnych potrzeb pracy.
* powinien posiadać wbudowane wysokiej jakości materiały do wykorzystania w pracy oraz wszechstronne zasoby edukacyjne dostępne z poziomu produktu.
* posiadać funkcję wyszukiwania i filtrowania czcionek
* posiadać narzędzie do rozdzielania obiektów wektorowych, tekstu oraz map bitowych wzdłuż dowolnej ścieżki.
* posiadać narzędzie do retuszowania zdjęć,
* posiadać narzędzie do klonowania korygującego w
* posiadać narzędzie do korygowania zniekształcenia perspektywy
* posiadać narzędzie do możliwość dostosowania obszaru roboczego projektowania do preferencji użytkownika np. dzięki opcjom niestandardowych rozmiarów ikon, kolorów pulpitu i obramowania okna.
* posiadać narzędzie do tworzenia logotypów, materiałów marketingowych, grafiki do witryn internetowych
* posiadać możliwość odczytu najpopularniejszych formatów plików graficznych
* posiadać możliwość rysowania symetrycznego, cień blokowy wyrównanie i rozkład węzłów, korektę perspektyw, pogląd i edycje krzywych, podgląd wektorowy, efekt perspektywy.

## System do zarządzania majątkiem (1 szt.)

System powinien zapewniać w pełni automatyczne przygotowanie i rozliczenie inwentaryzacji środków trwałych, wartości niematerialnych i prawnych oraz wyposażenia. Umożliwia prowadzenie ewidencji, amortyzacji składników majątku oraz sprawne zarządzanie posiadanymi aktywami.

Minimalne parametry systemu:

* Prowadzenie ewidencji wyposażenia, wartości niematerialnych i prawnych oraz majątku trwałego jednostki.
* Automatyczne generowanie numerów inwentarzowych.
* Generowanie planu amortyzacji na cały okres użytkowania.
* Naliczenie różnych typów amortyzacji (bilansowej, podatkowej).
* Porównanie stanu rzeczywistego majątku z prowadzoną ewidencją.
* Automatyczne wskazanie niedoborów/nadwyżek i ich przyczyn.
* Możliwość rozliczenia osób materialnie odpowiedzialnych za powierzone im mienie.
* Porównanie stanu rzeczywistego majątku z prowadzoną ewidencją.
* Generowanie niezbędnych dokumentów związanych z przychodem i rozchodem mienia, tj. dokumentów: OT, PT, LT, MT, WT oraz stanu składników majątku, tabeli amortyzacyjnej, wydruku pomocniczego do sprawozdania GUS F-03.
* Integracja z czytnikiem lub kolektorem kodów kreskowych.

## Mysz bezprzewodowa (30 szt.)

Minimalne parametry:

* Optyczny sensor
* Połączenie bezprzewodowe
* Interjejs: USB, radio 2,4 GHz
* Zasilanie bateryjne

## Dysk zewnętrzny (2 szt.)

* 256-bitowe szyfrowanie sprzętowe AES, płynne szyfrowanie wszystkich danych na dysku w czasie rzeczywistym
* Wbudowana pamięć – Minimum 2TB
* Wbudowana klawiatura do wprowadzania kodów dostępu (do 12 cyfr)
* Możliwość używania z telewizorem (funkcja niedostępna w przypadku dysków z normalnym szyfrowaniem)
* USB 3.1 GEN 1 (dostępny również z USB 3.0 / USB 2.0)
* Kontrolki LED zasilania / stanu szyfrowania
* Nie zapisuje haseł na komputerze ani w pamięci ulotnej systemu, dzięki czemu jest to rozwiązanie znacznie bezpieczniejsze od szyfrowania programowego
* Zgodność z komputerami PC i Mac

## Urządzenie wielofunkcyjne (3 szt.) – typ1

1) Prędkość drukowania (mono i w kolorze) A4: minimum 36 str./min.

2) Czas nagrzewania: do 16 s.

3) Rozdzielczość: optyczna 1200 x 1200 dpi, interpolowana 9600 x 600 dpi

4) Procesor: minimum 1,6 GHz

5) Interfejsy: 10Base-T, 100Base-TX, 1000Base-T, USB 2.0 (urządzenie i host), USB 3.0 (urządzenie i host), NFC, Bluetooth

6) Obsługiwane protokoły i porty: TCP/IP(IPv4, IPv6), LPR, Raw Port 9100, IPP1.0, FTP, HTTP, SMB (v1.0, v2.0, v2.1, v3.0,v3.1.1), POP3, SMTP, SSL, TLS (1.0, 1.1, 1.2, 1.3), SNMP V1, SNMP V3

7) Języki opisu strony: PCL6, Adobe PostScript3

8) Czujnik ruchu wykrywający zbliżającego się użytkownika

9) Pamięć: minimum 5 GB

10) Twardy dysk: standard 256 GB SSD/ opcja 512 GB SSD

11) Złącze wifi IEEE802.11 a/b/n/g/ac w standardzie

12) Panel sterowania: dotykowy, kolorowy , 10-calowy, ruchomy

13) Zoom: 25-400% w krokach co 1%

14) Kolorowe skanowanie sieciowe

15) Pojemność podajnika dokumentów: 300 ark. (80 g/m2)

16) Formaty dokumentów obsługiwane przez podajnik dokumentów: A6-A3, formaty użytkownika od 51 x 89 mm do 297 x 432 mm

17) Gramatura obsługiwana przez podajnik dokumentów: 35-220 g/m2

18) Prędkość skanowania: minimum 280 str./min.

19) Kasety na papier: na 550 ark. (80 g/m2)

20) Co najmniej 2 kasety obsługujące format papieru A5 – SRA3

21) Obsługiwana gramatura papieru w kasetach: 60 – 300 g/m2

22) Maksymalna gramatura dla wydruków w dupleksie: 256 g/m2 (z kaset i podajnika bocznego)

23) Podajnik boczny na 100 arkuszy (80 g/m2) obsługujący gramaturę 55 – 300 g/m2 i formaty A6-SRA3, formaty użytkownika od 90 x 140 mm do 320 x 457 mm oraz papier banerowy o wymiarach do 320 mm x 1300 mm

24) Sortowanie z przesunięciem dla formatów A4 i A3

25) Pojemność tacy odbiorczej: 400 ark. (80 g/m2)

26) Możliwość instalacji 2 dodatkowych tac odbiorczych o łącznej pojemności 220 ark. (80 g/m2)

27) Możliwość rozbudowy o finiszer ze zszywaniem (zszywanie dwupozycyjne, ręczne, bezzszywkowe)

28) Wbudowany moduł OCR pozwalający skanować do formatów .xlsx, .docx,. pptx, przeszukiwalny PDF

29) Wydruk plików z nośnika pamięci USB, w tym plików PDF, szyfrowany PDF, JPEG, TIFF, .xlsx, .pptx, . docx, PNG, PRN, TXT

30) Obsługa AirPrint, Microsoft Universal Print

31) Kopiowanie ciągłe: 1 – 9999

32) Czas maksymalny uzyskania pierwszej kopii: mono – 4,6 s., kolor – 6,5 s.

33) Bezpieczeństwo: wbudowany moduł TPM, opcjonalnie możliwość instalacji programu antywirusowego

34) Możliwość podglądu prac kopiowania / skanowania na panelu sterowania z możliwością edycji (zmiana kolejności stron, obracanie stron, usuwanie stron, strefowe usuwanie treści) przed zatwierdzeniem pracy

35) Drukowanie i kopiowanie w tandemie (praca zostanie rozłożona na dwa urządzenia)

36) Skanowanie do e-maila, FTP, SMB, do nośnika pamięci USB, na pulpit, na twardy dysk, sieciowy TWAIN

37) Możliwość skanowania do: TIFF, JPEG, PDF, PDF/A-1a, PDF/A-1b, szyfrowany PDF, XPS, przeszukiwalny PDF, pptx, docx, xlsx, JPEG, Compact PDF

38) Skanowanie wizytówek do formatu .vcf

39) Pomijanie pustych stron przy skanowaniu

40) Podział skanowanego dokumentu na oddzielne pliki o określonej ilości stron

41) Możliwość założenia 1000 folderów użytkowników na twardym dysku

42) Funkcja wydruku podążającego dla 10 urządzeń

43) System automatycznego wysuwania tonera – pojemnik z tonerem zostanie automatycznie wysunięty, gdy zostanie wyczerpany

44) Obsługa S/MIME, IEEE 802.1X

45) Nadpisywanie danych na twardym dysku

46) Możliwość instalacji aplikacji zewnętrznych dostawców

47) Funkcja zdalnego panelu – możliwość wyświetlenia panelu na ekranie komputera i wprowadzania ustawień oraz pracy na urządzeniu korzystając z tak wyświetlonego panelu.

48) Możliwość rozbudowy o moduł podłączenia do drugiej sieci komputerowej (łącznie ze skonfigurowaną funkcją skanowania do e-maila dla obydwu sieci).

49) Szyfrowanie danych algorytmem AES 256-bit

50) Obsługa oprogramowania typu SIEM

51) Obsługa serwisów w chmurze (skanowanie/drukowanie): One Drive for Business, Google Drive, Box, Dropbox, Sharepoint Online, MS Teams

52) Menu w języku polskim

53) Maksymalny pobór mocy 2,00 kW (AC 220-240 V/8 A, 50/60 Hz)

## Urządzenie wielofunkcyjne (2 szt.) – typ 2

|  |  |
| --- | --- |
| Funkcje urządzenia | Drukarka  Kopiarka  Skaner |
| Rodzaj druku | Laserowy kolor |
| Format | A4 |
| Parametry skanowania | Rozdzielczość 1.200 x 1,200dpi (z szyby skanera),  600 x 600dpi (ADF) |
| Parametry kopiowania | Szybkość kopiowania kolor A4 18 kopii na minutę |
| Prędkość druku | 15 str/min |
| Druk dwustronny | automatyczny |
| Podajnik papieru | 250 arkuszy  ADF - 50 arkuszy |
| Ethernet | 10/100 Mb/s |
| Złącza | 1 x USB 2.0 |
| Gwarancja | 2 lata |

## Niszczarka dokumentów (2 szt.)

1. Stopień bezpieczeństwa wg DIN 66399 P-4, T-4, E-3, F-1
2. Ilość jednorazowo ciętych kartek A4/80g. - 10
3. Rodzaj cięcia - ścinki limitowane
4. Szybkość cięcia min. 90mm./sek.
5. Głośność max. 57dB.
6. Szerokość szczeliny wejściowej min. 240mm
7. Wyposażona w hartowane stalowe wałki tnące wykowane z jednego elementu stali, separatory metalowe
8. Automatyczny oraz ręczny rewers w przypadku zakleszczenia papieru
9. Automatyczny start/stop za pomocą fotokomórki
10. System oszczędzania energii z max. Poborem energii w trybie stand-by 0,1W.
11. System termicznego zabezpieczenia przed uszkodzeniem urządzenia.
12. Osłona otworu wpustowego zapobiegająca przypadkowemu wciągnięciu części garderoby
13. Silnik indukcyjny o mocy min. 440W przystosowany do pracy ciągłej przez minimum 8 godzin.
14. Kosz o pojemności min. 33L wyjmowany z obudowy. Obudowa kosza pyłoszczelna
15. Gwarancja min. 36 miesięcy na urządzenie oraz dożywotnio na wałki tnące

## Słuchawki nauszne (15 szt.)

* Łączność przewodowa
* System audio stereo 2.0
* Pasmo przenoszenia słuchawek 20 ~ 20000 Hz
* Impedancja słuchawek 32 Om
* Czułość słuchawek 96 dB
* Wbudowany mikrofon
* Czułość mikrofonu -42dB
* Złącze minijack

## Komputery stacjonarne z monitorami (5szt.)

|  |  |
| --- | --- |
| **Podzespół** | **Minimalne parametry** |
| 1. Typ komputera | **Komputer stacjonarny** |
| 2. Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do zasobów lokalnej sieci komputerowej oraz usług sieci Internet, aplikacji graficznych wektorowych oraz rastrowych, a także danych multimedialnych. |
| 3. Procesor | klasy x86, 6 rdzeniowy, ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych, zapewniający wydajność min. 17600 pkt. w teście Passmark CPU Mark, znajdujący się na liście <https://www.cpubenchmark.net/cpu_list.php> |
| 4. Płyta główna | * chipset dostosowany do oferowanego procesora lub równoważny * minimum 4 sloty pamięci 3200 MT/s * minimum 1 x PCI Express 4.0 x 16 * minimum 1 x PCI Express 3.0 x 4 * minimum 5 złącz SATA 6.0 Gb/s * minimum 1x M.2 dla dysku SSD o przepustowości 64Gbit/s * minimum 1x M.2 dla dysku SSD o przepustowości 32Gbit/s * 1x USB (gniazdo bezpośrednio na płycie głównej) |
| 5. Pamięć operacyjna RAM | * minimum 8GB GB DDR4 * minimalny rozmiar możliwego rozszerzenia obsługiwanej pamięci, zapewniony  i potwierdzony przez producenta komputera: 128 GB |
| 6. Porty w tylnej części komputera | Komputer musi posiadać:   * minimum 2 x Display Port 1.4 z obsługą funkcji Multi-Stream, * możliwość zainstalowania trzeciego interfejsu wideo bez konieczności dokładania zewnętrznych kart graficznych; * minimum 6 x USB, w tym co najmniej 2x USB 3.2 Gen 1 * minimum 1 port sieciowy RJ-45, * Możliwość wyprowadzenia 1x port szeregowy (RS-232) – opcja rozbudowy, * osobne porty audio line-in i line-out   Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| 6. Porty w przedniej części komputera | Komputer musi posiadać:   * minimum 4 x USB-A, w tym min. 1x USB 3.2 Gen 2 * minimum 1 x USB -C 3.2 Gen 2 z obsługą Display port i Power Delivery * port audio do podłączenia słuchawek z mikrofonem |
| 7. Dysk twardy | * Minimum 256GB SSD z interfejsem M.2 NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego zainstalowanego  na komputerze przez producenta, po awarii, do stanu fabrycznego (tryb OOBE dla systemu MS Windows) * Możliwość zamontowania w obudowie jednego dysku 3,5 cala lub dwóch dysków 2,5 cala. |
| 8. Napęd optyczny | Nagrywarka DVD +/-RW |
| 9. Karta dźwiękowa | Karta dźwiękowa zintegrowana z płytą główną, zgodna ze standardem High Definition 5.1 |
| 10. Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.5, OpenCL 2.1. Możliwość fabrycznego zainstalowania dodatkowej, dedykowanej karty graficznej z pamięcią własną min. 4 GB. Grafika zintegrowana w procesorze musi umożliwiać jednoczesną obsługę co najmniej trzech monitorów. Na potrzeby obsługi większej liczby monitorów oferowany komputer musi umożliwiać jednoczesną obsługę monitorów podłączonych do grafiki zintegrowanej w procesorze oraz zainstalowanej osobnej karty graficznej (jeśli jest ona wymagana). |
| 11. Karta sieciowa | Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL oraz PXE. Zintegrowana karta sieciowa musi być wyposażona w diodę statusu informującą a aktywności połączenia oraz diodę informującą o prędkości połączenia. |
| 12. 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 |
| 13. Klawiatura | Klawiatura USB w układzie polskim programisty (105 klawiszy) z kablem o długości min. 1,8 m. |
| 14. Mysz | Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m. |
| 15. Obudowa | * Typu desktop (SFF) przystosowana do pracy w pionie i w poziomie, z obsługą kart PCI Express wyłącznie o niskim profilu; * Wbudowany głośnik do odtwarzania plików multimedialnych. * Suma wymiarów obudowy, nie może przekroczyć: 700 mm, najkrótszy z wymiarów nie większy niż: 90 mm * Możliwość zainstalowania wewnętrznego filtra przeciwkurzowego; * Obudowa jednostki centralnej beznarzędziowa, pozwalająca na demontaż komponentów i kart rozszerzeń (PCIe) oraz napędu optycznego i dysków twardych (co najmniej 3,5 cala) bez użycia narzędzi, z obiegiem powietrza tylko przód-tył - brak perforacji na bokach obudowy . * Głośność jednostki centralnej nie może przekraczać 21 dB, mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego. Wymagany raport badawczy, wystawiony przez niezależną, akredytowaną, co najmniej dla norm ISO 7779 i ISO 9296 jednostkę badawczą. |
| 16. Zasilanie | Zasilacz o mocy 280 W, o sprawności 92% przy obciążeniu 50%. |
| 17. Bezpieczeństwo i funkcje zarządzania | 1. Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. 2. Zamek zatrzaskowy z kluczem, nie wystający poza obrys obudowy zabezpieczający przed niepowołanym dostępem do wnętrza obudowy. 3. TPM 2.0. 4. Możliwość wbudowania czytnika SmartCard 5. Certyfikowane oprogramowanie umożliwiające – bez względu na stan czy obecność systemu operacyjnego w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego metodą 35 przebiegową - w ofercie należy podać nazwę i producenta oprogramowania. 6. 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) |
| 18. 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 i instalowanie aktualizacji).  Oprogramowanie 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. |
| 19. 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. |
| 20. Zainstalowane oprogramowanie systemowe | Zainstalowany system operacyjny w polskiej wersji językowej wraz z nośnikiem instalacyjnym  Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  *Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.*  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 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. 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. Obsługa standardu 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:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 27. Mechanizmy wieloelementowego uwierzytelniania. 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 30. Wsparcie dla algorytmów Suite B (RFC 4869). 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 36. 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. 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 40. Udostępnianie modemu. 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 43. 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.). 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie  z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 47. 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. 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
| 21. Gwarancja – zgodnie z wymaganiami i kryteriami | 36 miesięcy świadczonej w siedzibie Zamawiającego, przyjazd certyfikowanego przez producenta serwisanta do końca następnego dnia roboczego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym  - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej.  Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela |

### Monitor 27” (5 szt.)

|  |  |
| --- | --- |
| Ekran | 27 cali o rozdzielczości natywnej minimum 1920x1080 pikseli, maksymalny rozmiar piksela 0.275 mm, matryca matowa, pokryta powłoką 3H, technologia matrycy IPS |
| Parametry obrazu | Odwzorowanie 16.7 miliona kolorów, kontrast typowy 1000:1, jasność min. 250 cd/m2, czas reakcji matrycy max. 5ms, kąty widzenia pionowe/poziome minimum 178/178 stopni, 99% pokrycia przestrzeni kolorów sRGB |
| Wejścia wideo i inne | 1x DP 1.2, 1x HDMI 1.4, 1x D-SUB, wejście/wyjście audio, HUB USB 3.2 - 4 portowy |
| Obudowa i  regulacja monitora | Pochylenie ekranu w zakresie -5° / +35°(tzw. Tilt), funkcja Pivot, zintegrowany zasilacz i głośniki stereo o mocy minimum 2W każdy, złącze Kensington Lock, złącze montażu na ścianie w standardzie VESA |
| Funkcje zarządzana energią i parametrami wyświetlania obrazu | Technologia zapewniająca zużycie energii przez monitor w trybie power save na poziomie poniżej 0.2W pozwalająca na redukcję ogólnego zużycia energii przez monitor (bez konieczności manualnego wyłączania monitora przez użytkownika), zgodność z normą Energy Star 8.0, zużycie energii przy ustawieniach EPA max. 13W |
| Menu monitora | Regulacja głośności  Regulacja jasności  Regulacja kontrastu  Regulacja koloru (5000K, 6500K, 7500K, Użytkownika (R,G,B)  Menu w języku polskim oraz angielskim. |
| Kable | kabel sygnałowy cyfrowy o długości minimum 1.8m, kabel zasilający o długości minimum 1,8m, kabel audio |
| Gwarancja | Gwarancja 36 miesięcy |
| Certyfikaty i normy, dokumentacja | -Klasa energetyczna C  -TCO  -Epeat Silver  -TÜV Low Blue Light Certified  -TÜV Flicker Free Certified  -CE  -ISO9241-307(klasa I)  -RoHS, WEEE  -Instrukcja obsługi monitora |

## Komputery AIO (5 szt.)

* Typ: Komputer AIO. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
* Zastosowanie: Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
* Wydajność obliczeniowa: Procesor, który powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: <http://www.passmark.com/products/pt.htm>) co najmniej wynik 8700punktów Passmark CPU Mark.
* Pamięć operacyjna: minimum 8 GB 2933 MHz
* Parametry pamięci masowej: Min. 256 GB SSD NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.
* Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access).

Obsługująca funkcje:

- 4K przy 60Hz

- DirectX 12

- OpenGL 4.5

- Częstotliwość podstawowa układu graficznego 350 MHz

- Maksymalna częstotliwość dynamiczna układu graficznego 1.10 GHz

* Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
* Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition Audio. Obudowa wyposażona we wbudowane głośniki stereo.
* Obudowa
  + Typu AIO wyposażona w min. 1x kieszeń 2,5 cala na dyski SATA .
  + Wbudowany zasilacz o mocy minimum 190 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 93% przy 50-procentowym obciążeniu oraz 93%, przy 100-procentowym obciążeniu.
  + Obudowa musi mieć możliwość zabezpieczenia wnętrza komputera oraz wszystkich slotów znajdujących się z tyłu obudowy przed niepowołanym odstępem za pomocą kłódki lub linki typu Kensington.
* Ergonomia:
  + Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, która może blokować również dostęp do wnętrza komputera poprzez blokowanie klap serwisowych.
  + Ciężar komputera nie powinien przekraczać 11 kg.
* Wymagania dodatkowe
  + Zainstalowany system operacyjny w polskiej wersji językowej wraz z nośnikiem instalacyjnym.
  + Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.
  + Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.
  + System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
  + 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
  + a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
  + b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.
  + 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.
  + 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. Obsługa standardu 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:
  + a. Login i hasło,
  + b. Karty z certyfikatami (smartcard),
  + c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
  + 27. Mechanizmy wieloelementowego uwierzytelniania.
  + 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.
  + 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.
  + 30. Wsparcie dla algorytmów Suite B (RFC 4869).
  + 31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
  + 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
  + 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
  + 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
  + 35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
  + 36. 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.
  + 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
  + 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
  + 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
  + 40. Udostępnianie modemu.
  + 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
  + 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
  + 43. 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.).
  + 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
  + 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie
  + z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
  + 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
  + 47. 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.
  + 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
  + 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
  + 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.Dodatkowe, darmowe oprogramowanie pozwalające na w pełni  automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu
  + Wbudowane porty minimalnie:   
    - 1 x Display Port 1.2  
    - 1 x Audio: line-in/microphone  
    - 1 x Audio: line-out/headphone

- 1 x Audio front  
- 2x USB 3.2 Gen1 oraz USB-C 15 Watt z przodu obudowy

- 3x USB 2.0 oraz 1x USB 3.2 Gen1 z tyłu obudowy  
Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.

* + Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną.
  + Karta sieciowa WLAN Wi-Fi 6 z Bluetooth 5.1.
  + Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.
  + Minimum 2 złącza DIMM z obsługą do 64 GB DDR4 pamięci RAM.
  + Min. 2  złącza SATA NCQ AHCI w tym minimum 1 złącze SATA III 6 Gb/s.
  + Złącze M.2 PCIe 3.0; o przepustowości 32Gbit/s;
  + Złącze M.2-2230
  + Minimum jedna zatoka 5,25 cala (dopuszcza się zatokę na napędy typu SLIM) umożliwiająca instalację napędu optycznego. Zainstalowany napęd DVD-RW.
  + Specyfikacja wbudowanego ekranu::
    - Typ ekranu: Panoramiczny,  matryca o rozmiarze 23,8 cala
    - Jasność: 250 cd/m2
    - Kąty widzenia: 178°/178° CR10:1
    - Czas reakcji matrycy: maks. 14 ms
    - Rozdzielczość maksymalna: 1920 x 1080
    - Możliwość co najmniej 4-stopniowej regulacji wysokości ekranu w zakresie co najmniej 110 mm;
    - Możliwość obracania ekranu na boki w zakresie co najmniej 340°
    - Zakres pochylenia monitora: Od 0° do +20°
    - Konstrukcja komputera powinna umożliwić demontaż stopy ekranu i powieszenie komputera np. na ścianie za pomocą standardowego złącza VESA (100x100)
  + Klawiatura i mysz wyprodukowana przez producenta komputera
  + Zintegrowana z obudową monitora kamera
  + Zintegrowany mikrofon stereo cyfrowy
* Normy i standardy
  + Komputery mają spełniać normy  i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie:
    - Deklaracja zgodności CE
    - Być wykonane/wyprodukowane w systemie zapewnienia jakości  ISO 9001
* Gwarancja jakości producenta:
  + 36 miesięcy świadczonej  w siedzibie Zamawiającego, przyjazd certyfikowanego przez producenta serwisanta do końca następnego dnia roboczego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym
  + Naprawy gwarancyjne  urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta,
* Wsparcie techniczne producenta
  + Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
  + Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.

## Laptop Typ 1 (2 szt.)

|  |  |
| --- | --- |
| Zastosowanie | Zastosowanie: Komputer przenośny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Przekątna i rozdzielczość ekranu | Ekran o przekątnej > 15" o rozdzielczości FHD, matryca matowa AG o podwyższonej trwałości, kontrast 1000:1, jasność 300cd/m2. |
| Wydajność | * Procesor klasy x86, * Wydajność obliczeniowa: Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: <https://www.cpubenchmark.net/cpu_list.php>) co najmniej wynik 10800 punktów Passmark CPU Mark, na dzień 17.06.2022 lub nowszy. |
| Pamięć RAM | Pamięć operacyjna: minimum 16GB DDR4 3200 MHz możliwość rozbudowy do min 64 GB |
| Pamięć masowa | Parametry pamięci masowej: minimum 512GB SSD NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access). Obsługująca funkcje: DirectX 12, OpenGL 4.5, 4K@60Hz |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji. |
| Bezpieczeństwo | Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O.  Złącze typu Kensington Lock lub równoważne,  Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej TPM 2.0.  Wbudowany czytnik biometryczny – o parametrach minimum FAR (False Accept Rate) : nie większy niż, 0.00008%, FRR (False Reject Rate) : nie większy niż 0.01% . |
| Multimedia | Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki.  Dwa cyfrowe mikrofony wbudowane w obudowie matrycy  Kamera internetowa HD trwale zainstalowana w obudowie matrycy oraz dioda LED. Fabryczna zasłona obiektywu kamery. |
| Klawiatura | Klawiatura wyspowa układ US –QWERTY z wydzielonym blokiem klawiatury numerycznej.  *Dwustopniowe podświetlenie klawiatury.*  Touchpad wyposażony w dwa niezależne klawisze funkcyjne ze wsparciem dla technologii multitouch. Musi pozwalać na obsługę gestów dla minimum trzech niezależnych punktów dotyku. |
| Bateria i zasilanie | Min. 4-cell, 65 Wh, Li-Po Czas pracy na baterii minimum 12 godzin według dokumentacji producenta laptopa. Szybkie ładowanie baterii do 80% w czasie nie dłuższym niż 60 minut. Zasilacz o mocy min. 65W obsługujący ładowanie po porcie USB-C. |
| Waga i wymiary | Waga nie więcej niż: 1,55 kg  Grubość laptopa po złożeniu powinna być większa niż 19 mm. |
| Obudowa | Szkielet i zawiasy notebooka wykonane z wzmacnianego metalu. Obudowa laptopa powinna umożliwiać łatwą wymianę dysku, pamięci RAM oraz baterii przez użytkownika bez potrzeby interwencji serwisu - po demontażu klapy serwisowej. |
| Certyfikaty | Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 Professional 64-bit.  Deklaracja zgodności CE lub równoważne (załączyć do oferty)  Zgodność z: EnergyStar 8.0, TCO 8.0, EPEAT® Silver, WEEE, RoHS;  Zgodność z normą MIL-STD-810H  Oferowane laptopy muszą być wykonane/wyprodukowane w systemie zapewnienia jakości  ISO 9001 i ISO 14001 |
| Inne | Notebook musi być zgodny z następującymi technologiami:   * WMI (Windows Management Instrumentation) * PXE (Preboot Execution Environment) * WOL (Wake on LAN) * DMI (Desktop Management Interface) * SMBIOS (System Management BIOS) * CIM (Common Information Model) |
| BIOS | Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:   * Modelu komputera. * Nr seryjnego komputera. * Wersji BIOS (z datą). * Modelu procesora wraz z informacjami o prędkości taktowania * Informacji o ilości, typie i obsadzeniu pamięci RAM. * Informacji o dysku twardym: model oraz pojemność * MAC adresie zintegrowanej karty sieciowej * Numerze matrycy   Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB  Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie systemu, administratora i dysku twardego.  Możliwość autoryzacji użytkownika za pomocą technologii biometrycznej z poziomu BIOS przed uruchomieniem systemu operacyjnego |
| Dodatkowe oprogramowanie | Oprogramowanie dostarczone przez producenta komputera współpracujące np.  z Microsoft SCCM, pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej:   * + - Informowanie administratora o otwarciu obudowy     - Zdalne wyłączanie, restart oraz hibernacje komputera w sieci,     - Otrzymywanie informacji WMI – Windows Management Interface,     - Tworzenie raportów stanu jednostki,     - Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS,     - Aktualizację BIOS do najnowszej wersji zarówno dla pojedynczej maszyny jak i grupy,     - Tworzenie kopii zapasowych BIOS wraz z ustawieniami     - Tworzenie indywidualnych numerów dla poszczególnych użytkowników,     - Włączenie lub wyłączanie BOOTowania portów USB   Oprogramowanie umożliwiające w pełni  automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu.  Certyfikowane narzędzie zaimplementowane w BIOS komputera umożliwiające w bezpieczny (bezpowrotny) sposób usunięcie danych z dysku twardego bez względu na stan czy obecność systemu operacyjnego, obsługujące kasowanie 7 oraz 35 przebiegowe. |
| System operacyjny | Zainstalowany system operacyjny w polskiej wersji językowej wraz z nośnikiem instalacyjnym  Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.  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.  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. Obsługa standardu 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:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  27. Mechanizmy wieloelementowego uwierzytelniania.  28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.  29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.  30. Wsparcie dla algorytmów Suite B (RFC 4869).  31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.  32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.  33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.  35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,  36. 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.  37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.  38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.  40. Udostępnianie modemu.  41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  43. 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.).  44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).  45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie  z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.  46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.  47. 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.  48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.  49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.  50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
| Porty i złącza | * + - Min. 2 x USB 4.0 Gen3 zgodne z Thunderbolt 4.0     - Min. 3 x USB 3.2 Gen1 (przynajmniej jedno z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera).     - HDMI 2.0b     - Czytnik kart multimedialnych (SD, SDHC, SDXC)     - Audio port Combo (in-out)     - Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną z diodą sygnalizują status     - Zintegrowana w postaci wewnętrznego modułu karta WiFi 6, 802.11ax     - Notebook musi posiadać wbudowane gniazdo na kartę SIM oraz anteny.     - Bluetooth v 5.1,     - Dedykowane złącze do stacji dokującej (nie dopuszcza się USB – nawet dedykowanego), |
| Gwarancja | Gwarancji jakości producenta:   * + 60 miesięcy,   + Naprawy gwarancyjne  urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta,   + Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela   + Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera. |

## Laptop Typ 2 (19 szt.)

|  |  |
| --- | --- |
| Zastosowanie | Zastosowanie: Komputer przenośny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. Komputer musi być nowy i pochodzić z oficjalnego kanału dystrybucji |
| Przekątna i rozdzielczość ekranu | Ekran o przekątnej 15,6" o rozdzielczości FHD WLED (1920x1080) i jasności co najmniej 250 cd/m2, matryca matowa AG. Metalowe, wzmacniane zawiasy. |
| Wydajność | Procesor klasy x86 ze zintegrowaną grafiką, zapewniający równoważną wydajność całego oferowanego laptopa (Rating) min. 5000 pkt w teście Passmark CPU Mark 10 wg wyników dostępnych na stronie: <https://www.cpubenchmark.net/high_end_cpus.html>  Wynik nie starszy niż 3 miesiące od daty publikacji postępowania. |
| Pamięć RAM | Pamięć operacyjna: 8 GB z możliwością rozbudowy do min 64 GB, możliwość łatwej wymiany pamięci po odkręceniu pojedynczej śruby – bez konieczności demontowania laptopa. Przynajmniej jeden slot do rozbudowy pamięci RAM wolny. |
| Pamięć masowa | Parametry pamięci masowej: dysk SSD M.2 NVMe o pojemności min. 256GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. |
| Karta graficzna | Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.0, HLSL shader model 5.1 |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętow  ego wsparcia wirtualizacji) |
| Bezpieczeństwo | Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O.  Złącze typu Kensington Lock lub równoważne,  Zintegrowany z płytą główną układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej zgodne z TPM 2.0. |
| Multimedia | Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki;  Min. 1 cyfrowy mikrofon wbudowany w obudowie matrycy.  Kamera internetowa co najmniej HD (co najmniej 720p, 30 klatek na sekundę) trwale zainstalowana w obudowie matrycy, wyposażona w diodę LED sygnalizująca działanie kamery.  Wbudowany napędu optyczny w obudowę notebooka – co najmniej nagrywarka DVD-RW |
| Klawiatura | Klawiatura wyspowa układ US –QWERTY odporna na zachlapanie, minimum 104 klawisze z wydzielonym blokiem klawiatury numerycznej.  Touchpad wyposażony w dwa niezależne klawisze funkcyjne. |
| Bateria i zasilanie | Min. 3-cell, 45 Wh, Li-Ion. Czas pracy na baterii minimum 10 godzin według dokumentacji producenta laptopa. Możliwość łatwej wymiany baterii po odkręceniu jeden śruby. Zasilacz o mocy min. 65 W |
| Waga i wymiary | Waga nie więcej niż: 2 kg  Grubość laptopa po złożeniu powinna być mniejsza niż 24 mm. |
| Obudowa | Szkielet i zawiasy notebooka wykonane z wzmacnianego metalu. Możliwość wymiany pamięci RAM, dysku i baterii przez użytkownika – bez konieczności wizyty serwisie i bez konieczności rozbierania laptopa – dostępna klapa serwisowa wymagająca odkręcenia jedynie pojedynczej śruby. |
| Certyfikaty | Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 64-bit.  Norma EnergyStar 8.0 - komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov oraz [http://www.eu-energystar.org](http://www.eu-energystar.org/) lub może to potwierdzić inny dokument od producenta sprzętu potwierdzający spełnianie przez oferowany sprzęt wymaganej normy.  Oferowane laptopy muszą być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 14001. |
| BIOS | Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:  Modelu komputera.  Nr seryjnego komputera.  Wersji BIOS (z datą).  Modelu procesora wraz z informacjami o prędkości taktowania.  Informacji o ilości i typie pamięci RAM.  Informacji o dysku twardym: producent i model oraz pojemność  Informacja o napędzie optycznym (modelu napędu optycznego)  MAC adresie zintegrowanej karty sieciowej  Numerze matrycy  Możliwość wyłączenia/włączenia bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.:   * + - karty sieciowej RJ45     - karty sieciowej WLAN z Bluetooth     - kamery     - portów USB     - czytnika kart multimedialnych     - kontrolera audio     - głośników     - mikrofonu     - zintegrowanej funkcjonalności TPM   Funkcja blokowania/odblokowania BOOT-owania z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB  Możliwość włączenia/wyłączenia hasła dla dysku twardego,  Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie użytkownika, administratora i dysku twardego. |
| Dodatkowe oprogramowanie | Oprogramowanie umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu. |
| System operacyjny | Zainstalowany system operacyjny w polskiej wersji językowej wraz z nośnikiem instalacyjnym  Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.  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.  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. Obsługa standardu 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:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  27. Mechanizmy wieloelementowego uwierzytelniania.  28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.  29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.  30. Wsparcie dla algorytmów Suite B (RFC 4869).  31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.  32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.  33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.  35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,  36. 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.  37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.  38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.  40. Udostępnianie modemu.  41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  43. 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.).  44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).  45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie  z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.  46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.  47. 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.  48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.  49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.  50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
| Porty i złącza | * + - RJ-45 (nie dopuszcza się stosowania adapterów)     - Min. 1x UB 3.2 Gen2 typu USB-C z możliwością ładowania baterii laptopa oraz wyprowadzenia sygnału Display Port     - Min. 3x USB 3.2 Gen1 (1 z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera nawet przy wyłączonym laptopie).     - HDMI w wersji co najmniej 1.4     - Czytnik kart multimedialnych (SD, SDHC i SDXC)     - Audio: port combo mikrofon/słuchawki     - Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną.     - Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11ac z dwiema antenami.     - Zintegrowana karta WLAN musi zapewniać możliwość bezprzewodowego bezpośredniego (t.j. bez pośrednictwa punktu dostępowego lub sieci LAN) podłączenia do komputera dodatkowego monitora lub projektora wyposażonego w odpowiedni adapter (lub natywną obsługę takiej funkcji) z wykorzystaniem standardów IEEE 802.11n w pasmie 2,4 GHz lub 5GHz, w trybie ekranu systemowego – z obsługą wyświetlania w trybie klonowania ekranów, rozszerzonego desktopu oraz wyświetlania ekranu systemu jedynie na dodatkowym monitorze lub projektorze (Clone, Extended Desktop, Remote Only).     - Wymagana jest obsługa przesyłania dowolnej treści ekranu oraz dźwięku systemu operacyjnego z parametrami nie gorszymi niż:     - • rozdzielczość 1920x1080 - 30 fps–kompresja H.264     - • dźwięk AC3 5.1 Surround Audio     - • obsługa szyfrowania WPS/WPA2/WEP     - Bluetooth co najmniej w standardzie v5.0, |
| Gwarancja | Gwarancji jakości producenta:   * + Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca,   + Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta notebooka   + Zgłoszenia serwisowe drogą online (formularz online producenta notebooka) , telefonicznie oraz mailem |

## Serwer plików (1 szt.)

|  |  |
| --- | --- |
| Procesor | Czterordzeniowy o taktowaniu co najmniej 2,2GHz np. AMD Ryzen V1500B |
| Architektura procesora | 64-bitowy x86 |
| Koprocesor arytmetyczny | Tak |
| Obudowa | Rack 2U o wymiarach nie większych niż: 90(H) x 484(W) x 300 (D) mm |
| Pamięć RAM | 4GB SODIMM DDR4, możliwość rozszerzenia pamięci RAM do 64GB |
| Pamięć flash | 5GB |
| Ilość obsługiwanych dysków | 8 dysków 3,5-calowych SATA 6Gb/s  2 dyski SSD M.2 NVMe 2280 |
| Zainstalowane dyski | 3 dyski o pojemności min. 4TB znajdujące się na liście zgodności producenta NAS |
| Interfejsy sieciowe | 2 x 2,5GbE (RJ45) |
|  |
| Gniazdo  PCIe | 1 x PCIe Gen3 x8 |
| Porty USB | 2 x USB Typu-C 3.2 Gen 2 (10Gb/s)  2 x USB Typu-A 3.2 Gen 2 (10Gb/s) |
| Wskaźniki LED | HDD, Stan, LAN, USB, zasilanie |
| Obsługa RAID | Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60 |
| Funkcja Hot Spare | RAID Hot Spare and Global Hot Spare |
| Szyfrowanie | Możliwość szyfrowania folderów i wolumenów kluczem AES 256-bit. |
| Wspierane Systemy Operacyjne | 1. Apple Mac OS 10.10 or later 2. Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux 3. IBM AIX 7, Solaris 10 or later UNIX 4. Microsoft Windows 7, 8, and 10 5. Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019 |
| Protokoły | CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu  Windows ACL  Integracja w Windows ADS  Serwer WWW  Serwer plików  Manager plików przez WWW  Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI  Replikacja w czasie rzeczywistym  Serwer RADIUS  Klient LDAP  Serwer Syslog  Container Station |
| Zarządzanie dyskami | Skanowanie w poszukiwaniu złych sektorów, odczyt S.M.A.R.T |
| Język GUI | Polski |
| Waga | Max. 11 kg |
| System plików | Dyski wewnętrzne ZFS, EXT4.  Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Zasilanie | Redundantne (2x 300W) |
| Wentylatory | Min. 3 x 60 mm |
| W zestawie | Szyny do montażu w szafie RACK |
| Gwarancja i serwis | 5 lat gwarancji na NAS  5 lat gwarancji na dyski |

## Serwer wirtualizacyjny (1 szt.)

|  |  |
| --- | --- |
| Obudowa | * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej; * Możliwość zainstalowania 10 dysków twardych hot plug 3,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane 2 szt. dysków SSD SATA 240GB hot-plug; * Zainstalowane 4 szt. dysków SATA 2TB hot-plug; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. |
| Płyta główna | * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji procesorów 38-rdzeniowych; * Zainstalowany moduł TPM 2.0; * 7 aktywnych złącz PCI Express generacji 4 w tym:   + 4 fizyczne złącza o prędkości x16;   + 3 fizyczne złącza o prędkości x8;   + Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;   + Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; * 32 gniazda pamięci RAM; * Obsługa minimum 4TB pamięci RAM DDR4; * Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + ECC   + Memory Mirroring   + ADDDC; * Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) * Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  nie zajmujące klatek dla dysków hot-plug; |
| Procesory | * Dwa procesory 8-rdzeniowe * Taktowanie 2,1GHz * architektura x86\_64   osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 139 pkt  (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/cpu2017.html> |
| Pamięć RAM | * 128 GB pamięci RAM * DDR4 Registered * 3200Mhz |
| Kontrolery LAN | * Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; |
| Kontrolery I/O | * Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache (opcjonalnie możliwość zabezpieczenia za pomocą baterii lub kondensatora) |
| Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 2 port USB 3.0 wewnętrzne; * 2 porty USB 3.0 dostępne z tyłu serwera; * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; * 2 porty USB 3.0 na panelu przednim |
| Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W; * Redundantne wentylatory hotplug; |
| Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express     - procesory CPU     - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM     - wbudowany na płycie głównej nośnik pamięci M.2 SSD     - status karty zrządzającej serwera     - wentylatory     - bateria podtrzymująca ustawienia BIOS płyty główne     - zasilacze   Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera;   + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Możliwość zarządzania przez 6 administratorów jednocześnie   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)   + Wsparcie dla protokołu SSDP   + Obsługa protokołów TLS 1.2, SSL v3   + Obsługa protokołu LDAP   + Integracja z HP SIM   + Synchronizacja czasu poprzez protokół NTP   + Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); * Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. * BIOS UEFI w specyfikacji 2.7; |
| Wspierane OS | * Microsoft Windows Server 2022, 2019, 2016 * VMWare vSphere 6.7, 7.0 * Suse Linux Enterprise Server 15 * Red Hat Enterprise Linux 7.9, 8.3 * Hyper-V Server 2016, 2019 |
| Gwarancja | * 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki; |
| Dokumentacja, inne | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; * Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; |
| System operacyjny | Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się aby oferowane licencje umożliwiały korzystanie 30 urządzeniom.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

## Oprogramowanie do backupu (1 szt.)

|  |  |
| --- | --- |
| L.p. | Nazwa |
| I | Wymagania minimalne |
| 1 | Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji |
| a | Microsoft Hyper-V min. w wersjach 2019, 2016, 2012R2, 2012 |
| b | Vmware vSphere min. w wersjach v4.1-7.0 |
| c | Nutanix AHV 5.10 (LTS) |
| d | Maszyny fizyczne: Windows Server 2019, 2016, 2012R2, 2012, 2008R2 |
| 2 | Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V |
| 3 | Oprogramowanie musi pozwalać na wdrożenie w środowiskach |
| a | na serwerze sprzętowym, obsługiwane systemy operacyjne w ramach: Windows Server 2008 R2 – 2019 (x64), Windows 7 – 10 Professional (x64), Ubuntu 16.04 – 18.04 Server (x64), Red Hat Enterprise Linux 7.4 – 7.6 (x64), SUSE Linux Enterprise Server 12 SP1-SP3 (x64), CentOS 7.6 |
| b | jako maszyna wirtualna Vmware |
| c | jako maszyna wirtualna Amazon |
| d | na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital |
| 4 | Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS |
| 5 | Oprogramowanie nie może wymagać instalacji jakiegokolwiek agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania |
| 6. | Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji (np. Frameworków czy baz danych) |
| II | Licencjonowanie |
| 1 | Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności |
| 2 | Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska |
| 3 | W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 5 lat wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania |
| 4 | W ramach dostawy wymagane jest dostarczenie licencji na ochronę 2 gniazd procesorów w hostach Vmware lub Hyper-V |
| 5 | Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska |
| III | Ochrona danych |
| 1 | Oprogramowanie musi posiadać funkcje backupu i replikacji: |
| a | Backup maszyn wirtualnych Vmware |
| b | Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu |
| c | Backup maszyn wirtualnych Hyper-V |
| d | Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu |
| e | Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych |
| f | Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie |
| g | Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu |
| h | Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym |
| i | Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych  Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem |
| j | Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania |
| IV | Optymalizacja wykorzystania miejsca na dane |
| 1 | Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych: |
| a | Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane |
| b | Kompresja backupu, w tym konfigurowalny stopień kompresji |
| c | Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne |
| V | Spójność danych |
| 1 | Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych: |
| a | Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux |
| b | Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu |
| c | Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: |
|  | Microsoft Exchange 2013, 2016, 2019 |
|  | Microsoft SQL 2008, 2008R2, 2012, 2014, 2016, 2017, 2019 |
| d | Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki |
| e | Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V |
| f | Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania |
| g | Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji |
| VI | Przywracanie danych |
| 1 | Oprogramowanie musi posiadać poniższe funkcje: |
| a | Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji |
| b | Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) |
| c | Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej) |
| d | Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): |
|  | Microsoft Exchange |
|  | Active Directory |
|  | MS SQL |
| e | Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie. |
| VII | Wydajność |
| 1 | Oprogramowanie do backupu musi pozwalać na: |
| a | Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT |
| b | Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych |
| c | Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN |
| d | Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci |
| VIII | Zarządzanie |
| 1 | Oprogramowanie musi pozwalać na następujące formy zarządzania: |
| a | Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych |
| b | Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej |
| c | Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania |
| d | Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport. |
| e | Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji |

## Szafy do punktów dystrybucyjnych (4 szt.)

Szafa ma 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. Ponad to szafa powinna być wyposażona w dedykowany panel wentylacyjny dachowy, 2 wentylatorowy. Kolor szafy: czarny. Głębokość do 1000cm.

## UPS do szafek dystrybucyjnych (szt. 4)

Do zasilania urządzeń w szafie RACK, projektuje się zasilacz UPS wykonany w technologii podwójnej konwersji on-line (VFI).

Szafę RACK należy wyposażyć w zasilacz UPS o mocy 1kVA/0,9kW.

Wymaga się, aby instalowane zasilacze UPS wyposażone były w baterię podtrzymującą, która umożliwia ponowne uruchomienie UPS nawet w przypadku awarii głównego źródła zasilania - tzw. funkcja „Cold Start”.

Zasilacz UPS należy wyposażyć w następującą ilość akumulatorów:

• UPS 1 kVA – 1 gałąź bateryjna 2 akumulatory 9Ah – 12V umieszczone wewnątrz obudowy zasilacza.

Wymagania minimalne:

WEJŚCIE

• Napięcie nominalne 230V

• Częstotliwość 50/60Hz

• Zakres częstotliwości 40-70Hz

• Współczynnik mocy >0,99

WYJŚCIE:

• Współczynnik mocy PF 0,9

• Napięcie 230V

• Częstotliwość 50/60Hz

• Zniekształcenia harmoniczne <3% THD dla obciążenia liniowego

OGÓLNE:

• Funkcja „Cold Start” – uruchamianie zasilacza UPS z baterii

• Sposób montażu RACK 19” – wymagana możliwość zmiany orientacji wyświetlacza RACK/TOWER

• Styk EPO (awaryjne wyłączanie zasilania)

• Karta komunikacji LAN/SNMP – możliwość zdalnego zarządzania i monitorowania zasilacza UPS

• Maksymalne wymiary (Szer. x Gł. x Wys.) mm: 440x430x86,5 (2U)

• Funkcja “hot swap” bezprzerwowa wymiana baterii

• Podwójna konwersja online (VFI)

Zasilacze UPS należy instalować w szafie RACK używając dedykowanych szyn montażowych do RACK 19”. Zasilacz UPS należy wyposażyć w kartę komunikacji LAN/SNMP.

## Punkt dostępowy (8 szt.)

Punkt dostępowy o poniższych parametrach:

- musi mieć możliwość pracy z lokalnym kontrolerem WLAN lub być zarządzanym za pomocą rozwiązania znajdującego się w chmurze producenta przy czym zmiana trybu pracy nie może odbywać się poprzez podmianę systemu operacyjnego urządzenia (firmware);

- musi posiadać dwa niezależne moduły radiowe obsługujące 802.11ax (2.4 i 5 GHz);

- musi mieć możliwość pracy w trybie Dual 5G – dwa interfejsy radiowe pracujące jednocześnie w paśmie 5GHz;

- musi wspierać tryb OFDMA w obydwu zakresach częstotliwości (2,4 i 5 GHz);

- musi wspierać TxBF (Transmit Beamforming);

- musi wspierać indeksy od HE0 do HE11 dla obydwu częstotliwości radiowych (2,4 i 5 GHz);

- musi wspierać pracę w trybach co najmniej HE20/HE40/HE80 dla częstotliwości 5 GHz;

- musi wspierać pracę w trybach co najmniej HE20 dla częstotliwości 2,4 GHz;

- musi posiadać moduł Bluetooth (BLE) - IEEE 802.15.4;

- obsługa minimum 2x2 MIMO z modulacją 1024QAM;

- musi posiadać minimum 4 wbudowane anteny dookólne;

- zysk energetyczny anten musi wynosić minimum 2,5dBi dla 2,4GHz oraz 3,5dBi dla 5GHz;

- musi posiadać minimum 1 port RJ-45 pracujący w trybie autonegocjacji;

- musi posiadać port USB;

- musi umożliwiać uruchomienie 8 SSID per moduł radiowy (16 per AP);

- musi umożliwiać jednoczesne podłączenie 512 użytkowników per moduł radiowy (1024 per AP);

- musi posiadać funkcjonalność minimalizacji wpływu zakłóceń z sieci komórkowych CCF (Cellular Coexistence Filter);

- musi być wyposażony w firewall typu stateful (L2-L7);

- musi umożliwiać konfigurację 802.1x, 802.11i, WPA, WPA2;

- musi posiadać najnowszy standard bezpieczeństwa WPA3 dla zapewnienia najlepszej ochrony użytkowników i urządzeń IoT;

- musi posiadać wbudowany chip TPM;

- musi posiadać certyfikaty kompatybilności Wi-Fi Alliance (Wi-Fi CERTIFIED 6, Passpoint, WMM, WMM Power Save, Wi-Fi Agile Multiband oraz Protected Management Frames);

- musi posiadać fizyczny przycisk umożliwiający reset urządzenia;

- musi posiadać gniazdo pozwalające na mocowanie linki zwanej MicroSaver zabezpieczającej cenny sprzęt przed kradzieżą (Kensington Lock);

- musi posiadać minimalny zakres temperatur pracy 0-40°C;

- maksymalny pobór mocy urządzenia 11,5W (bez podłączonego USB);

- produkt musi być objęty dożywotnią gwarancją producenta rozumianą jako data zakończenia jego sprzedaży (EOS) + 5 lat. Podczas jej trwania klient ma możliwość wymiany uszkodzonego urządzenia z gwarancją wysyłki nowego przez producenta następnego dnia roboczego po akceptacji procedury RMA oraz możliwość zgłaszania problemów technicznych przynajmniej poprzez dedykowany portal WWW producenta. Ma również nieograniczony dostęp do dokumentacji technicznej.

## Przełącznik sieciowy (4 szt.)

Wymagania ogólne dla urządzeń typu Przełącznik dostępowy

1. Wysokość urządzenia 1U

2. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T

3. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.

4. Przełącznik musi posiadać wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.

5. Możliwość łączenia do 8 przełączników w stos z posiadanymi przez Zamawiającego przełącznikami Extreme Networks X440 i X620. Urządzenia połączone w stos muszą być widziane jako jedno logiczne urządzenie, zarządzanie z jednego adresu IP. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych

6. Tablica MAC adresów min. 16k

7. Pamięć operacyjna: min. 1GB pamięci DRAM

8. Pamięć flash: min. 4GB pamięci Flash oraz bufora pakietów min. 1,5MB

9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094

10. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)

11. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)

12. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.

13. Możliwość monitorowania zajętości CPU

Obsługa Routingu IPv4

14. Pojemność tabeli routingu min. 480 wpisów

15. Routing statyczny

16. Obsługa routingu dynamicznego IPv4

a. RIPv1/v2

b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

17. Policy Based Routing dla IPv4

Obsługa Routingu IPv6

18. Pojemność tabeli routingu min. 240 wpisów

19. Routing statyczny

20. Obsługa routingu dynamicznego dla IPv6

a. RIPng

b. Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv3 (np. poprzez dodatkową licencję)

21. Policy Based Routing dla IPv6

Obsługa Multicastów

22. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)

23. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping

Bezpieczeństwo

24. Obsługa Network Login

a. IEEE 802.1x

b. Web-based Network Login

c. MAC based Network Login

25. Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants)

26. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC

27. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login

28. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma

29. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:

a. definicji sieci VLAN,

b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,

c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,

d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.

30. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication

31. Bezpieczeństwo MAC adresów

a. ograniczenie liczby MAC adresów na porcie

b. zatrzaśnięcie MAC adresu na porcie

c. możliwość wpisania statycznych MAC adresów na port/vlan

d. możliwość wyłączenia MAC learning

32. Zabezpieczenie przełącznika przed atakami DoS

a. Networks Ingress Filtering RFC 2267

b. SYN Attack Protection

c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

33. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)

34. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation

35. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard

Bezpieczeństwo sieciowe

36. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania

37. Obsługa STP, RSTP, MSTP, PVST+

38. Obsługa EAPS (RFC 3619) oraz G.8032

39. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów

40. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

41. Zarządzanie przez SNMP v1/v2/v3

42. Obsługa SYSLOG z możliwością definiowania wielu serwerów

43. Sprzętowa obsługa sFlow

44. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)

Inne

45. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)

46. Możliwość uruchamiania skryptów

a. Ręcznie

b. O określonym czasie lub co wskazany okres czasu

c. Na podstawie wpisów w logu systemowym

47. Urządzenie musi być objęte dożywotnią gwarancją producenta obejmującą (z możliwym ograniczeniem do 5 lat od zaprzestania sprzedaży):

a. bezpłatne aktualizacje oprogramowania firmware,

b. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego od zgłoszenia awarii,

c. wsparcia technicznego producenta poprzez infolinię, pocztę e-mail oraz telefon.

Wymagania szczegółowe dla urządzeń typu Przełącznik dostępowy 48 portowy

Wszystkie zapisy ogólne dotyczące urządzeń typu Przełącznik dostępowy i dodatkowo:

1. Przełącznik posiadający 48 portów 1G 100/1000BASE-T

2. Przełącznik posiadający 8 portów 1G SFP (mogą być porty typu Combo)

3. Przełącznik mający możliwość rozbudowy (licencje – np. kosztem portów SFP, dodatkowy moduł) o 4 porty 10G SFP+.

4. Nieblokującą architekturę o wydajności przełączania min. 176 Gb/s

5. Szybkość przełączania min. 130 Milionów pakietów na sekundę

## Licencje na hosting usługi pocztowej (30 szt.)

* Licencja obejmująca terminową subskrypcję (min 12 miesięcy) konta pocztowego o rozmiarze minimum 50GB dla użytkownika, możliwość wysyłania załączników o rozmiarze 150MB
* 1TB magazynu w chmurze na użytkownika
* Możliwość korzystania z aplikacji biurowych w ramach licencji poprzez przeglądarkę internetową
* Platforma do organizowania oraz uczestniczenia w video-spotkaniach online dla 300 użytkowników

## Oprogramowanie biurowe (31 szt.)

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,

2. Wymagania odnośnie interfejsu użytkownika:

a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.

b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.

c. 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.

3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.

4 .Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.

5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:

a. posiada kompletny i publicznie dostępny opis formatu,

b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 do rozporządzenia 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 (Dz. U., poz. 526),

c. umożliwia wykorzystanie schematów XML,

d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.

7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.

8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).

9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:

a. Edytor tekstów

b. Arkusz kalkulacyjny

c. Narzędzie do przygotowywania i prowadzenia prezentacji

d. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)

e. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.

11. Edytor tekstów musi umożliwiać:

a. 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.

b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.

c. Wstawianie oraz formatowanie tabel.

d. Wstawianie oraz formatowanie obiektów graficznych.

e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).

f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

g. Automatyczne tworzenie spisów treści.

h. Formatowanie nagłówków i stopek stron.

i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.

j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.

k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.

l. Określenie układu strony (pionowa/pozioma).

m. Wydruk dokumentów.

n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.

o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.

p. Zapis i edycję plików w formacie PDF.

q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.

s. 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.

12. Arkusz kalkulacyjny musi umożliwiać:

a. Tworzenie raportów tabelarycznych

b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych

c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)

e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych

f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych

g. Wyszukiwanie i zamianę danych

h. Wykonywanie analiz danych przy użyciu formatowania warunkowego

i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie

j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności

k. Formatowanie czasu, daty i wartości finansowych z polskim formatem

l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

m. inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.

n. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).

o. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.. p. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

a. Przygotowywanie prezentacji multimedialnych, które będą:

b. Prezentowanie przy użyciu projektora multimedialnego

c. Drukowanie w formacie umożliwiającym robienie notatek

d. Zapisanie jako prezentacja tylko do odczytu.

e. Nagrywanie narracji i dołączanie jej do prezentacji

f. Opatrywanie slajdów notatkami dla prezentera

g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo

h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego

i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym

j. Możliwość tworzenia animacji obiektów i całych slajdów

k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.

l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

14. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,

b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,

c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,

d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,

e .Automatyczne grupowanie poczty o tym samym tytule,

f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,

g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,

h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,

i. Zarządzanie kalendarzem,

j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,

k. Przeglądanie kalendarza innych użytkowników,

l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,

m. Zarządzanie listą zadań,

n. Zlecanie zadań innym użytkownikom,

o. Zarządzanie listą kontaktów,

p. Udostępnianie listy kontaktów innym użytkownikom,

q. Przeglądanie listy kontaktów innych użytkowników,

r. Możliwość przesyłania kontaktów innym użytkowników,

s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

15. Oprogramowanie musi być dostarczone w najnowszej wersji

## Projektor multimedialny z ekranem ściennym (1 szt.)

|  |  |
| --- | --- |
| Technologia wyświetlania | DLP |
| Jasność | Co najmniej 4000 ANSI lumen – pomiar jasności zgodny z normą ANSI |
| Rozdzielczość natywna | 1920 x 1080 |
| Kontrast | Co najmniej 15 000:1 |
| Proporcje obrazu | Dokładnie 16:9 |
| Korekcja zniekształcenia trapezowego | Co najmniej +/-40 stopni w pionie |
| Współczynnik projekcji | Obejmujący swoim zakresem 1,40-1,65 |
| Maksymalna przekątna obrazu | Co najmniej 300” |
| Złącza wejściowe | Co najmniej:   * 1 x VGA * 2 x HDMI * Wejście audio niesymetryczne |
| Złącza wyjściowe | Co najmniej:   * 1 x VGA * 1 x audio niesymetryczne |
| Dodatkowe złącza | Co najmniej:   * 1 x RS-232 |
| Głośnik/i | Wbudowany/e, o mocy co najmniej 2W |
| Źródło światła | Lampa lub laser |
| Gwarancja producenta | Co najmniej 2 lata na sam projektor, dowolna na źródło światła – z zastrzeżeniem, że projektor musi zostać dostarczony ze źródłem światła tego samego producenta co sam projektor, jako komplet |
| Dodatkowa funkcjonalność | Co najmniej:   * Menu OSD projektora w języku polskim * Możliwość ustawienia blokady bezpieczeństwa/hasła dostępu |

Projektor musi zostać zamontowany za pomocą uchwytu sufitowego w wyznaczonym przez Zamawiającego miejscu.

Uchwyt sufitowy powinien posiadać:

* Możliwość pochylenia: w osi projektora + /- 15°, na boki +/- 22.5°
* Odległość od punktu mocowania: 43 - 65 cm

Ekran projekcyjny ścienny

|  |  |
| --- | --- |
| Typ ekranu | rozwijany elektrycznie |
| Szerokość ekranu | 200cm |
| Wysokość ekranu | 200cm |
| Szerokość obrazu | 190cm |
| Wysokość obrazu | 106.9cm |
| Przekątna obrazu | 85.8 cale |
| Czarne ramki boczne | 5cm |
| Czarny TOP | 88,1cm |
| Czarny dół | 4cm |
| Kąt widzenia | 160° |
| Rodzaj sterowania | ścienne + bezprzewodowe |
| Rodzaj silnika | Tubowy |
| Możliwość zabudowy w suficie | TAK |

## Projektor multimedialny z ekranem przenośnym (1 szt.)

|  |  |
| --- | --- |
| Technologia wyświetlania | DLP |
| Jasność | Co najmniej 4000 ANSI lumen – pomiar jasności zgodny z normą ANSI |
| Rozdzielczość natywna | 1920 x 1080 |
| Kontrast | Co najmniej 15 000:1 |
| Proporcje obrazu | Dokładnie 16:9 |
| Korekcja zniekształcenia trapezowego | Co najmniej +/-40 stopni w pionie |
| Współczynnik projekcji | Obejmujący swoim zakresem 1,40-1,65 |
| Maksymalna przekątna obrazu | Co najmniej 300” |
| Złącza wejściowe | Co najmniej:   * 1 x VGA * 2 x HDMI * Wejście audio niesymetryczne |
| Złącza wyjściowe | Co najmniej:   * 1 x VGA * 1 x audio niesymetryczne |
| Dodatkowe złącza | Co najmniej:   * 1 x RS-232 |
| Głośnik/i | Wbudowany/e, o mocy co najmniej 2W |
| Źródło światła | Lampa lub laser |
| Gwarancja producenta | Co najmniej 2 lata na sam projektor, dowolna na źródło światła – z zastrzeżeniem, że projektor musi zostać dostarczony ze źródłem światła tego samego producenta co sam projektor, jako komplet |
| Dodatkowa funkcjonalność | Co najmniej:   * Menu OSD projektora w języku polskim * Możliwość ustawienia blokady bezpieczeństwa/hasła dostępu |

Do projektora należy dostarczyć ekran projekcyjny przenośny, wyposażony w odpowiednią torbę transportową.

Ekran projekcyjny przenośny:

|  |  |
| --- | --- |
| Typ ekranu | Na trójnogu |
| Szerokość ekranu | 200cm |
| Wysokość ekranu | 200cm |
| Szerokość obrazu | 195cm |
| Wysokość obrazu | 195cm |
| Przekątna obrazu | 108 cale |
| Czarne ramki boczne | 2,5cm |
| Czarny TOP | 2,5cm |
| Czarny dół | 2,5cm |
| Kąt widzenia | 160° |

## Urządzenie firewall Typ 1

1) Zapora sieciowa typu Next Generation Firewall (NGFW),

2) Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.

3) Minimalna ilość interfejsów:

a) 8 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.

b) 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,

c) 1 interfejs konsoli do zarządzania zaporą,

4) Zapora powinna posiadać możliwość montażu dysku o pojemności przynajmniej 256 GB.

5) Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa

6) Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji,

7) Możliwość utworzenia przynajmniej 128 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q,

8) Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej,

9) Minimalna ilość jednocześnie obsługiwanych połączeń: 900 000,

10) Możliwość obsłużenia przynajmniej 9 000 nowych połączeń w ciągu 1 sekundy.

11) Przepustowość urządzenia pracującego w trybie stateful firewall: 3 Gbps – dla ramki 1518B zgodnie z RFC 2544,

12) Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1,5 Gbps,

13) Przepustowość urządzenia pracującego jako koncentrator VPN: 1,38 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544,

14) Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 1 Gbps,

15) Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 100,

16) Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 100

17) Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 5 z możliwością rozszerzenia do przynajmniej 200.

18) Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.

19) Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 500 Mbps oraz obsłużyć 30 000 połączeń.

20) Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,

21) Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),

22) Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),

23) Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP,

24) Wsparcie dla Dynamicznego DNS tzw. DDNS,

25) Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.

26) Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).

27) Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:

a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),

b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,

c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.

28) Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,

29) Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.

30) Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.

31) Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.

32) Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),

33) Kontrola dostępności zestawionych tuneli VPN,

34) Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.

35) Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.

36) Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić),

37) Funkcja NAT oparta o reguły bezpieczeństwa.

38) NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe),

39) Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.

40) Zintegrowany system skanowania antyspyware,

41) Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.

42) System IPS musi używać algorytmu szeregowego przetwarzania.

43) Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).

44) Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,

a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.

b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,

c) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.

45) System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.

46) Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,

47) Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,

48) Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,

49) Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń

50) Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.

51) Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.

Funkcjonalność nie może wymagać zakupu dodatkowych licencji.

52) Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 16 takich punktów dostępowych sieci bezprzewodowej.

53) Urządzenie dostarczone z elementami niezbędnymi do zamocowania w szafie RACK 19″.

Wszystkie wymagane do tego elementy muszą pochodzić od tego samego producenta.

1. Gwarancja: Min. 60 mc, wsparcie w trybie 24x7.

2. Wymagane licencje:

* Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 5 lat.

## Urządzenie firewall Typ 2 (2 szt.)

1) Zapora sieciowa typu Next Generation Firewall (NGFW),

2) Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.

3) Minimalna ilość interfejsów:

a) 8 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.

b) 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,

c) 1 interfejs konsoli do zarządzania zaporą,

4) Zapora powinna posiadać możliwość montażu dysku o pojemności przynajmniej 256 GB.

5) Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa

6) Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji,

7) Możliwość utworzenia przynajmniej 64 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q,

8) Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej,

9) Minimalna ilość jednocześnie obsługiwanych połączeń: 750 000,

10) Możliwość obsłużenia przynajmniej 6 000 nowych połączeń w ciągu 1 sekundy.

11) Przepustowość urządzenia pracującego w trybie stateful firewall: 2 Gbps – dla ramki 1518B zgodnie z RFC 2544,

12) Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1 Gbps,

13) Przepustowość urządzenia pracującego jako koncentrator VPN: 750 Mbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544,

14) Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 750 Mbps,

15) Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 50,

16) Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 50

17) Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 5 z możliwością rozszerzenia do przynajmniej 200.

18) Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.

19) Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 300 Mbps oraz obsłużyć 25 000 połączeń.

20) Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,

21) Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),

22) Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),

23) Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP,

24) Wsparcie dla Dynamicznego DNS tzw. DDNS,

25) Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.

26) Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).

27) Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:

a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),

b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,

c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.

28) Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,

29) Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.

30) Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.

31) Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.

32) Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),

33) Kontrola dostępności zestawionych tuneli VPN,

34) Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.

35) Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.

36) Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić),

37) Funkcja NAT oparta o reguły bezpieczeństwa.

38) NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe),

39) Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.

40) Zintegrowany system skanowania antyspyware,

41) Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.

42) System IPS musi używać algorytmu szeregowego przetwarzania.

43) Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).

44) Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,

a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.

b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,

c) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.

45) System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.

46) Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,

47) Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,

48) Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,

49) Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń

50) Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.

51) Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.

Funkcjonalność nie może wymagać zakupu dodatkowych licencji.

52) Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 16 takich punktów dostępowych sieci bezprzewodowej.

53) Urządzenie dostarczone z elementami niezbędnymi do zamocowania w szafie RACK 19″.

Wszystkie wymagane do tego elementy muszą pochodzić od tego samego producenta.

1. Gwarancja: Min. 60 mc, wsparcie w trybie 24x7.

2. Wymagane licencje:

Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 5 lat

## Skaner (1 szt.)

|  |  |
| --- | --- |
| **CECHA** | **Minimalne parametry** |
| Typ skanera | Skaner z automatycznym podajnikiem dokumentów ADF z wbudowanym podajnikiem płaskim A4 oraz możliwością późniejszej rozbudowy o dedykowany podajnik płaski formatu A3 (tego samego producenta). |
| Tryb skanowania | Skanowanie dwustronne jednoprzebiegowe (duplex); kolor/skala szarości/monochromatyczny |
| Przeznaczenie urządzenia | Skanowanie dokumentów o różnych formatach i gramaturach bez konieczności ich wcześniejszej segregacji, skanowanie dokumentów długich |
| Format skanowanych dokumentów | A3 i mniejsze |
| Ilość układów optycznych | 3 - możliwość skanowania w trybie duplex z ADF |
| Element światłoczuły dla ADF | CIS |
| Typ oswietlenia | LED |
| Prędkość skanowania dla 300DPI tryb cz&b, kolor i skala szarości | 60 arkuszy/min, 120 obrazów/min |
| Rozdzielczość optyczna | 600 DPI |
| Rozdzielczość wyjściowa | 100-1200 DPI |
| Panel kontrolny | 3.5 cala kolorowy dotykowy ekran LCD z możliwością predefiniowania profili skanowania i uruchamiania ich z poziomu skanera wraz z możliwością indywidualnego opisu zadań w języku polskim |
| Automatyczny podajnik dokumentów | regulowany, min. w 3 stopniach na 300 arkuszy o gramaturze 80g/m2 |
| Tryb skanowania kopert | skanowanie kopert i grubych dokumentów A3 przy użyciu ADF za pomocą prostej ścieżki prowadzenia papieru |
| Poprawa jakości skanowanych dokumentów dla sterowników Twain oraz ISIS | Likwidacja przekosu, automatyczne rozpoznawanie wielkości i rozmiaru dokumentu, usuwanie kolorów; skanowanie dwustrumieniowe kolor i czarno-biały za jednym przebiegiem; automatyczna rotacja dokumentu, automatyczne wykrywanie koloru, inteligentne wygładzanie koloru tła, inteligentne wypełnienie krawędzi obrazu, scalanie obrazów, wykrywanie pustych stron na podstawie procentowej zawartości oraz rozmiarze pliku, filtrowanie smug, filtr ostrości, układanie dokumentów na tacy wyjściowej, |
| Format pliku wyjściowego | Tiff, jpg, bmp, pdf,pdf/A, pdf przeszukiwalny do j. polskiego, rtf do j. polskiego, xml z wartością odczytanego kodu kreskowego |
| Format pliku indeksowego | Możliwość generowania pliku xml lub csv - zawierającego informację na temat liczby zeskanowanych stron, oraz wartości odczytanego kodu kreskowego np.: Interleaved 2 of 5, Code 3 of 9, Code 128, Codabar, UPC-A, UPC-E, EAN-13, EAN-8, PDF417, QR code |
| Wsparcie dla sterowników | TWAIN, ISIS oraz Linux |
| Interfejs komunikacyjny z PC | USB 3.2 lub szybszy, LAN 10/100/1000 wbudowany w urządzenie |
| Obciążenie dzienne | 25 000 skanów |
| Maksymalna wspierana przez skaner długość dokumentu | 4000 mm |
| Zakres gramatury skanowanych dokumentów dla ADF | 37–433 g/m² |
| Czujnik podwójnych pobrań dokumentów | ultrasonic z interaktywnym przywracaniem wykrycia wielu arkuszy |
| Ochrona dokumentów przed zgnieceniem za pomocą czujnika akustycznego | tak - z regulacją czułości z poziomu sterownika |
| Wspierane systemy operacyjne dla sterowników TWAIN oraz ISIS | Windows 7 SP1 (wersja 32-bitowa  i 64-bitowa), Windows 8 (wersja 32-bitowa i 64-bitowa), Windows 8.1 (wersja 32-bitowa i 64-bitowa), Windows 10 (wersja 32-bitowa i 64-bitowa), Windows Server 2012 x64, Windows Server 2016 x64, Windows Server 2019/2022 x64, Linux Ubuntu 18.04 |
| Gwarancja | 36 miesięcy |
| Waga | 20kg |
| Pobór mocy | tryb pracy <50W, tryb uśpienia <4W, tryb czuwania <0.3W |
| Deklaracja zgodności | CE |
| Ochrona Środowiska | Energy Star, EPEAT, ROHS. |
| Oświadczenia | - |

## Zestaw nagłośnieniowy (2 szt.)

Minimalne parametry:

* System 2.0
* Pilot w zestawie
* Max moc głośników 80W
* Pasmo przenoszenia min 50Hz
* Pasmo przenoszenia max 20kHz
* Stosunek sygnału do szumu 72dB
* Komunikacja Bluetooth
* Złącza: 3,5 mm minijack, AUX, 2 x S/PDIF
* Zasilanie sieciowe
* Obsługiwane kodeki: SBC
* Pilot zdalnego sterowania na podczerwień
* Listwa dźwiękowa jest zgodna z urządzeniami pamięci masowej USB o pojemności do 32 GB w formacie FAT32, Obsługuje wejście optyczne (do telewizora)
* Długość kabla:
* Kabel 3.5mm AUX-in: około 1,5 m
* Kabel od zasilacza AC około 1,5m
* Od prawej do lewej satelity Kabel o długości 2,0 m umocowany na lewym satelicie

## Cyfrowy odtwarzacz audiobooków (10 szt.)

Przenośny, cyfrowy odtwarzacz do słuchania audiobooków, muzyki, słuchowisk, podcastów, z dyktafonem.

Minimalne parametry techniczne odtwarzacza:

* pamięć wewnętrzna 16 GB
* obsługa kart SD o pojemności do 128 GB
* wbudowany głośnik o mocy min 1 W
* akumulator litowo-jonowy o pojemności min 3,4 Ah
* złącze słuchawkowe mini jack 3,5 mm, z możliwością podłączenia słuchawek lub zewnętrznego mikrofonu
* złącze mini USB, do ładowarki lub do podłączenia do komputera
* dedykowane złącze do ładowania akumulatora 9V
* zasilacz/ładowarka AC 230V / DC 9V 0,66 A
* klawiatura z cyframi i piktogramami
* min 3 lata gwarancji
* możliwość zapisania w pamięci urządzenia 190 godzin nagrań
* obsługiwane formaty:

- mp3, ogg, wav

## Mysz dla niepełnosprawnych (1 szt.)

W związku z przygotowywaniem stanowiska komputerowego dla osób niepełnosprawnych zamawiający przewiduje jedną mysz o poniższych parametrach:

* Trackball, dwuprzyciskowy dla osób prawo i leworęcznych
* instalacja za pomocą przewodowego połączenia USB, bez konieczności stosowania baterii

## Tablety (4 szt.)

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Parametry wymagane** |
| Typ | Urządzenie typu Tablet, w ofercie wymagane jest podanie modelu, symbolu oraz producenta tabletu |
| Zastosowanie | Tablet będzie wykorzystywany dla potrzeb aplikacji rozszerzonej rzeczywistości , dostępu do internetu. |
| Procesor | Minimalnie ośmiordzeniowy, minimalne taktowanie jednego rdzenia 1.8 GHz |
| Pamięć operacyjna | Co najmniej 4GB |
| Parametry pamięci masowej | Min. 64 GB . |
| Bateria i ładowanie | Akumulator o pojemności min. 5000mAh  Czas pracy baterii do 10 godzin przeglądania stron internetowych |
| Złącza | USB (typu-C lub mikro)  Czytnik kar pamięci MicroSD  Gniazdo słuchawek i mikrofonu |
| Wyposażenie multimedialne | Wbudowane głośniki stereo i dwa mikrofony |
| Standardy i certyfikaty | TÜV Rheinland Low Blue Light  RoHS compliant |
| Obudowa/ wyświetlacz | 1. Matryca o przekątnej min 10” i rozdzielczości min. 1280x800 pikseli, 400nits, w technologii IPS. 2. Na obudowie muszą być trwale naniesione następujące dane urządzenia: nazwa lub logo producenta |
| Warunki gwarancji | Min 1 rok |
| Komunikacja bezprzewodowa | WiFi 802.11 a/b/g/n/ac  Wi-Fi Direct  Bluetooth min 5.0  4G LTE |
| Wymagania dodatkowe | Tablet musi posiadać: Akcelerometr, żyroskop, moduł GPS, czujnik natężenia światła otoczenia, czujnik Halla, wbudowana kamera przednia o minimalnej rozdzielczości 5MP, wbudowana kamera tylna o minimalnej rozdzielczości 8MP. |

## Zasilacz UPS do serwerowni (1 szt.)

Wymaga się, aby zasilacz UPS wyposażony były w baterię podtrzymującą, która umożliwia ponowne uruchomienie UPS-a nawet w przypadku awarii głównego źródła zasilania - tzw. funkcja „Cold Start”.

Projektowany zasilacz UPS należy wyposażyć w następującą ilość akumulatorów:

•UPS 3kVA – 1 gałąź bateryjna 6 akumulatorów 9Ah – 12V, zainstalowane wewnątrz obudowy zasilacza UPS.

Wymagania minimalne:

WEJŚCIE

• Napięcie nominalne 230V

• Częstotliwość 50/60Hz

• Zakres częstotliwości 40-70Hz

• Współczynnik mocy >0,99

WYJŚCIE:

• Współczynnik mocy PF 0,9

• Napięcie 230V

• Częstotliwość 50/60Hz

• Zniekształcenia harmoniczne <3% THD dla obciążenia liniowego

OGÓLNE:

• Funkcja „Cold Start” – uruchamianie zasilacza UPS z baterii

• Sposób montażu RACK 19” – wymagana możliwość zmiany orientacji wyświetlacza RACK/TOWER

• Styk EPO (awaryjne wyłączanie zasilania)

• Karta komunikacji LAN/SNMP – możliwość zdalnego zarządzania i monitorowania zasilacza UPS

• Maksymalne wymiary (Szer. x Gł. x Wys.) mm: 440x720x86,5 (2U)

• Funkcja “hot swap” bezprzerwowa wymiana baterii

• Podwójna konwersja online (VFI)

Zasilacz UPS należy instalować w szafie RACK (minimalna głębokość szafy 800mm, optymalna 1000mm) używając dedykowanych szyn montażowych do RACK 19”. Zasilacz UPS należy wyposażyć w kartę komunikacji LAN/SNMP.

## Wdrożenie

### Firewall

1. Montaż urządzeń szafie rack oraz
2. Nadanie adresu IP
3. Konfiguracja dostępu SSH
4. Zmiana haseł dostępu
5. Aktualizacja oprogramowania do najnowszej możliwej wersji
6. Stworzenie do 500 reguł bezpieczeństwa
7. Konfiguracja tuneli VPN (Site-to-Site i Client-to-Site), po stronie wykonawcy będzie instalacja odpowiednich klientów VPN na komputerach użytkowników
8. Konfiguracja routingu
9. Utworzenie polityk bezpieczeństwa
10. Wdrożenie funkcjonalności DPI
11. Wdrożenie deszyfracji protokołu SSL
12. Stworzenie klastra wysokiej dostępności
13. Przepisanie konfiguracji VLAN z obecnego rozwiązania firewall
14. Konfiguracja firewall, reguły przychodzące i wychodzące na podstawie obecnie działających usług
15. Konfiguracja ochrony przed malware, exploitami oraz stronami zawierającymi złośliwy kod
16. Uruchomienie i konfiguracja systemu do zbierania logów z systemu firewall
17. Wdrożenie PKI oraz konfiguracja polityki za pomocą których przeprowadzona zostanie dystrybucja certyfikatów.
18. Rekonfiguracja wykorzystywanych przeglądarek www przez zamawiającego do pracy z włączoną deszyfracją protokołu SSL na firewall.
19. Transfer wiedzy do klienta na temat obsługi zaproponowanej konfiguracji

### Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:

a) przeprowadzić testy poprawności działania całej infrastruktury

b) przygotować dokumentację powykonawczą zawierająca listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów

c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

* urządzenia dedykowane (embeded), na przykład routery i przełączniki;
* punkty styku z sieciami obcymi
* zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
* Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:
* określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
* wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;
* Badaniu będą podlegały następujące systemy:
* rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
* Linux 2.4.x, 2.6.x, 3.x.x;
* IBM AIX;
* CISCO IOS;
* Microsoft SQL;
* MySQL;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez Zamawiającego przed zakończeniem projektu.

### Wymagania w zakresie **Firewall.**

Zamawiający wymagać będzie na etapie realizacji zamówienia, aby prace związane z instalowaniem, konfiguracją i wdrażaniem instalacji Firewall wykonywały osoby posiadające stosowne umiejętności w tym zakresie. Powyższe prace musza wykonywać osoby:

* 1. posiadające wiedzę i doświadczenie w zakresie implementacji środowisk sieciowych i systemowych opartych na posiadanych przez Zamawiającego platformach Microsoft Server, obejmujące instalowanie i konfigurowanie elementów systemów oraz wiedzę i doświadczenie w zakresie zarządzania tymi środowiskami i rozwiązywania dotyczących ich problemów, obejmujące administrowanie systemami i obsługę ich użytkowników przy spełnieniu wymagań dla Microsoft Certified Solutions Associate (MCSA) lub wymagań równoważnych, tj., określonych na nie niższym poziomie jakości, potwierdzone certyfikatem Microsoft Certified Solutions Associate (MCSA) lub innym równoważnym dokumentem (zaświadczeniem);
  2. posiadające wiedzę i doświadczenie w zakresie definiowania i charakteryzowania najważniejszych technik ataków stosowanych przez hakerów oraz identyfikowania i analizowania podatności na ataki hakerów w organizacji a także w tworzeniu polityki na urządzeniach IDS/IPS dotyczącej wykrywania włamań, spełniającej wymagania dla Certified Ethical Hacker (CEH) lub inne równoważne, tj. określone na nie niższym poziomie jakości niż CEH, potwierdzone certyfikatem ukończeniem szkolenia Certified Ethical Hacker (CEH) lub innym tożsamym dokumentem (zaświadczeniem),
  3. posiadające wiedzę i doświadczenie z zakresu tworzenia skryptów i programów w języku Python na posiadanym przez zamawiającego oprogramowaniu lub systemach operacyjnych. Przy użyciu praktyk spełniających wymagania dla PCAP - Certified Associate in Python Programming lub inne równoważne, tj. określone na nie niższym poziomie jakości niż PCAP - Certified Associate in Python Programming, potwierdzone certyfikatem PCAP - Certified Associate in Python Programming lub innym równoważnym dokumentem (zaświadczeniem),
  4. posiadające certyfikat inżynierski z zakresu konfiguracji i rozwiązywania problemów na zaproponowane rozwiązanie Firewall

Wykonawca (lub jego podwykonawca) przed przystąpieniem do prac instalacyjnych przedłoży Zamawiającemu dokumenty potwierdzające że osoby wymienione