Załącznik nr 1 do SWZ

Szczegółowy opis przedmiotu zamówienia

1. Wstęp

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia na dostawę sprzętu oraz oprogramowania.

2. Przedmiot zamówienia

a) dostawa fabrycznie nowego Sprzętu wraz z oprogramowaniem;
b) udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego na dostarczony Sprzęt;
c) dostarczenie przez Wykonawcę Dokumentacji dostarczonego Sprzętu na etapie dostarczania Sprzętu do siedziby Zamawiającego.

3. Termin realizacji zamówienia oraz liczba dostarczanego Sprzętu i Oprogramowania i szkoleń

a) Zamawiający wymaga, aby dostawa Sprzętu i Oprogramowanie, o których mowa w pkt 3 do Zamawiającego nastąpiła w terminie 90 dni, liczonych od dnia zawarcia umowy.
b) Na przedmiot zamówienia składają się:

Lp.	Nr części	Przedmiot zamówienia	j.m.	ilość	Okres gwarancji
1	Cześć 1	**Serwer rack z systemem i licencjami dostępowymi**	szt.	2	Gwarancja minimum 36 miesięcy
2		**Przełącznik sieciowy 48 portowy**	szt.	3	
3		**Oprogramowanie do backupu serwerów**	szt.	2	
4	Część 2	**Serwer NAS typ 1**	szt.	1	Gwarancja minimum 12 miesięcy
5		**Serwer NAS typ 2**	szt.	1	
6		**Serwer NAS typ 3**	szt.	1	
7		**Urządzenie bezpieczeństwa sieciowego**	szt.	1	
8		**Monitor interaktywny z uchwytem ściennym**	szt.	4	
9		**Notebook typ 1**	szt.	16	
10		**Notebook typ 2**	szt.	3	
11		**Oprogramowanie antywirusowe- pakiet edukacyjny – 50 licencji**	szt.	1	
12		**Kamera internetowa**	szt.	3	
13		**Słuchawki**	szt.	2	
14		**Dysk zewnętrzny**	szt.	2	
15		**Pamięć typu pendrive**	szt.	3	

4. Wymagania ogólne

Numer wymagania	Opis wymagania
1	Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację, możliwość uruchomienia oraz użytkowanie w typowym środowisku, np. przewody zasilające i zasilacz, niezbędne uchwyty, szyny.
2	Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez

	Zamawiającego z tych rozwiązań w takiej funkcji jednakże w każdym przypadku nie krócej niż przez czas w jakim będzie technicznie możliwe używanie Sprzętu.
3	Dokumenty gwarancyjne wystawiane lub przekazywane przez Wykonawcę powinny być zgodne z OPZ oraz z zapisami zawartymi we wzorze umowy.

5. Kryteria równoważności

Numer wymagania	**Opis wymagania**
1	W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
2	W sytuacjach, kiedy Zamawiający opisuje szczegółowy przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisane, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
3	Pod pojęciem rozwiązań równoważnych Zamawiający rozumie takie Oprogramowanie, które w równoważnym stopniu spełnia warunki określone w SOPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany udowodnić w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 ustawy Pzp, że proponowane przez niego rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
4	Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SOPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

6. Wymagania szczegółowe

6.1 Serwer rack z systemem i licencjami dostępowymi– 2 szt.

Parametr	**Minimalne wymagania**
Typ	Serwer

Zastsowanie	Przeznaczony do zadań serwerowych, praca ciągła (24/7/365/), wirtualizacja, przechowywanie, udostępnianie zasobów.
Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Ramię porządkujące ułożenie przewodów z tyłu serwera; • Możliwość zainstalowania min. 16 dysków twardych hot plug 2,5"; • Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; • Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

Płyta główna	• Min. Dwuprocesorowa;
	• Wyprodukowana i zaprojektowana przez producenta serwera
	• Możliwość instalacji procesorów 40-rdzeniowych;
	• Zainstalowany moduł TPM 2.0;
	• Min. 6 złącz PCI Express generacji 4 w tym:
	  ○ Min. 4 fizyczne złącza o prędkości x16;
	  ○ Min. 2 fizyczne złącza o prędkości x8;
	  ○ Opcjonalnie możliwość uzyskania min. 4 złącz typu pełnej wysokości;
	• Min. 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 nie zajmujące klatek dla dysków hot-plug;

Procesory	• Minimum jeden procesor 16-rdzeniowy, • taktowanie bazowe min. 2,4GHz • architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 269 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html
Pamięć RAM	• minimum 128 GB pamięci RAM w modułach po min. 32 GB • DDR4 Registered • Minimum 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 2x10Gbit oraz 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; • Dodatkowa karta sieciowa na zainstalowana w slocie PCIe z interfejsami 2x

	10Gbit SFP+
Dyski twarde	• Zainstalowane 2 szt. dysków SSD SATA 480GB o DWPD min. 1,5; • Zainstalowane 3 szt. dysków SSD SATA 960GB o DWPD min. 5;
Kontrolery I/O	• Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe; • Zainstalowany kontroler SAS RAID obsługujący poziomy RAID min. 0,1,10,5 zapewniający obsługę wszystkich 16 wnęk na dyski w serwerze
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu oraz przodu serwera; • Min. 2 porty USB 3.0 wewnętrzne; • Min. 2 porty USB 3.0 dostępne z tyłu serwera; • Możliwość instalacji portu serial i jego wykorzystania 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; • Min. 2 porty USB 3.0 na panelu przednim
Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimalnej 900W; • Redundantne wentylatory hotplug;
Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii o 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 pełne zarządzanie, zdalny restart serwera; o Dedykowana karta LAN min. 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; o Dostęp poprzez przeglądarkę Web, SSH; o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; o Zarządzanie alarmami (zdarzenia poprzez SNMP) o Możliwość przejęcia konsoli tekstowej o Możliwość zarządzania przez min. 6 administratorów jednocześnie o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) o 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.
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
System	Minimalne wymagania co do licencji do serwerowego systemu operacyjnego: min. 1 szt. licencji wieczystej Microsoft Windows Server 2022 Standard (16 Core) lub system równoważny (do każdego dostarczanego serwera) Minimalne wymagania: obsługa technologi COM, .NET, posiadający możliwości zarządzania komputerami z systemem Microsoft Windows 10 / Windows 11 oraz użytkownikami i uprawnieniami do zasobów na poziomie identycznej funkcjonalności jak usługa katalogowa Active Directory w systemach Windows Server firmy Microsoft, w tym przede wszystkim dotyczącej uwierzytelniania i autoryzacji użytkowników, Licencjonowanie musi uwzględniać dostarczanie przez producenta oprogramowania poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania i prawo do bezpłatnej ich instalacji w okresie przynajmniej 5 lat od daty publikacji oprogramowania przez producenta tego oprogramowania i co najmniej 4 lata od dostawy oprogramowania przez wykonawcę. Licencjonowanie musi uwzględniać automatyczne dostarczanie przez producenta oprogramowania poprawek. w ramach dostępnej licencji umożliwiający implementację co najmniej 2 maszyn wirtualnych. wsparcie dla wizualnej, identycznej do wbudowanej w systemach firmy Microsoft

	usługi zdalnego pulpitu: Remote Desktop Services (RDS), system kompatybilny z oprogramowaniem dziedzinowym używanym w urzędzie, które oparte jest o bazy danych Microsoft SQL Server Express (64-bit) w wersji 15.x lub wyższej oraz system zarządzania relacyjnymi bazami danych Firebird w wersji co najmniej 2.5.x, obsługa w ramach usługi katalogowej rozbudowanych polityk bezpieczeństwa – polityk dla systemów operacyjnych komputerów będących w domenie lokalnej, użytkowników i ewentualnie dla określonych aplikacji,
Licencje dostępowe typu User CAL	Minimalne wymagania co do licencji dostępowej User CAL do systemu Microsoft Windows Server 2022 lub równoważnego : 50 szt. licencji wieczystej MS Windows Server 2022 User CAL 2022 lub równoważnej, tj. • licencja dostępowa przypisana do użytkownika, • dostęp do serwera przez licencjonowanych użytkowników w celu korzystania z usług, takich jak przechowywanie plików, drukowanie i innych usług systemu MS Windows Server 2022 lub równoważnego, (50 szt. dotyczy sumarycznej ilości licencji dostępowej dostarczanej z serwerami)
Gwarancja	• Min. 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 ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • 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;
Dodatkowe prace	1. Instalacja w szafie RACK, podłączenie okablowania oraz niezbędna konfiguracja dwóch serwerów fizycznych.

Opis równoważności dla systemu Windows Server 2022 Standard:
*równoważne tj. spełniające poniższe warunki:
1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencje na system operacyjny musi pozwalać na zainstalowanie przez Zamawiającego systemu na szesnastu fizycznych serwerach z 1 fizycznym procesorem z 4 rdzeniami każdy zgodnie z polityką licencjonowania producenta oprogramowania.
7. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
8. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
9. System operacyjny musi posiadać graficzny interfejs użytkownika.
10. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
a. zarządzania użytkownikami,
b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
c. możliwości przydzielania praw dostępu do zasobów sieciowych,
d. instalacji zdalnej oprogramowania z pakietów msi, e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1,10,11.
11. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
12. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center .
13. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
14. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
15. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
16. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra 34. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.

19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
22. System operacyjny musi posiadać obsługa PowerShell 5.1,
23. System operacyjny musi posiadać obsługa certyfikatów w Active Directory
24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

6.2 Przełącznik sieciowy 48 portowy – 3 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Typ	Przełącznik sieciowy Ethernet Smart Management rack 1Gbit. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Porty	a) Minimum 48 porty 1G RJ45 10/100/1000BASE-T b) Minimum 4 porty SFP+ z możliwością pracy 1G/10G Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX
3.	Parametry fizyczne	Wysokość maksymalnie 1U, montowany w szafie typu rack 19''
4.	Pamięć	Co najmniej 512 MB SDRAM Co najmniej 256 MB pamięci flash Bufor pakietów co najmniej 1.5 MB
5.	Wielkość tablicy adresów MAC	Co najmniej 16000
6.	Ilość obsługiwanych sieci VLAN	Co najmniej 256
7.	Wydajność	• Przepustowość przełączania: min. 176 Gbit/s • Przełączanie dla pakietów: min. 130.95 Mpps. • Opóźnienie: < 4.5 uSec dla 100 Mb < 2.2 uSec dla 1000 Mb <1.2 uSec dla 10 Gbps
8.	Obsługa ramek Jumbo	O wielkości co najmniej 9216 bajtów

9.	Funkcjonalność urządzenia	• obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad), • wsparcie da LLDP oraz LLDP-MED • obsługa protokołu SNTP, • Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s) • Minimum 256 obsługiwanych sieci VLAN • Minimum 50 możliwych do utworzenia list ACL, • CoS zgodna z 802.1p • Voice VLAN • Minimum 509 wpisów ARP • Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy • Port Security • DHCP Snooping • Klient Radius • Port mirroring, • DHCP Relay, • DoS Protection, • ARP Attack Protection, • Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu
10.	Zasilanie	Zasilacz 230V AC wbudowany,
11.	Temperatura pracy	0°C do 40°C
12.	Maksymalny pobór mocy	36.9 W
13.	Wentylacja	bezwentylatorowy
14.	Zarządzanie	WWW (GUI), SNMP Manager, cloud-based web portal
15.	Akcesoria	Kabel zasilający
16.	Gwarancja	Min. 36 miesięcy Produkty są objęte 90-dniowym całodobowym telefonicznym wsparciem technicznym. Przez pozostały okres gwarancji, dostępne będzie tylko wsparcie techniczne za pomocą czatu. Ograniczona gwarancja dożywotnia, obowiązuje tak długo, jak produkt jest używany przez pierwszego właściciela, dodatkowo jest ograniczona do pięciu (5) lat od daty wycofania produktu ze sprzedaży Dostęp do wersji oprogramowania przez cały okres posiadania dotyczy wszystkich ogólnodostępnych wersji oprogramowania / systemów operacyjnych dla wymienionych produktów, gdy i jeśli są dostępne, przez cały okres posiadania produktu przez klienta
17.	Dokumenty	Urządzenie musi posiadać deklaracja zgodności CE.

6.3 Oprogramowanie do backupu serwerów – licencja na procesory – 2 szt.

Parametr	Minimalne wymagania
Ogólne	1. Oprogramowanie może być dostarczane w dwóch scenariuszach: a. Cloud(Software as Service), b. On-premise.

	2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud. 3. Interfejs systemu dostępny jest w języku: a. polskim, b. angielskim, 4. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych, 5. Oprogramowanie może być uruchomione w kontenerze docker, 6. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: a. Debian: 9+ b. Ubuntu: 16.04+ c. Fedora: 29+ d. centOS: 7+ e. RHEL: 6+ f. openSUSE: 15+ g. SUSE Enterprise Linux (SLES): 12 SP2+ h. Windows Client: 7, 8.1, 10 (1607+) i. Windows Server: 2008 R2+, 7. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, 8. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),

Wsparcie techniczne:	1. Pomoc techniczna w językach: a. polskim, b. angielskim. 2. Materiały samopomocowe: a. Baza wiedzy: ■ polski, ■ angielski
Zarządzanie:	1. Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli dostępnej z poziomu przeglądarki internetowej, 2. Zarządzanie całym systemem poprzez dashboardy, 3. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, 4. System posiada wbudowane predefiniowane zadania backupowe, 5. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. 6. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, 7. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, 8. Monitorowanie postępu działania zadania, 9. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: a. Zadanie zostało zakończone pomyślnie, b. Zadanie zostało zakończone z ostrzeżeniami, c. Zadanie zostało zakończone z błędem, d. Zadanie zostało anulowane, e. Zadanie nie zostało uruchomione. 10. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego. 11. Możliwość zdefiniowania okna backupowego dla każdego z zadań, 12. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów, 13. System pozwala na klonowanie planów kopii zapasowych, 14. System umożliwia reset hasła administratora w przypadku jego utraty, 15. Oprogramowanie umożliwia definiowanie retencji według schematów: a. GFS(Grandfather-Father-Son), b. FIFO(First-In, First-Out). 16. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami, 17. Konta użytkowników mogą być tworzone poprzez import pliku CSV, 18. Oprogramowanie umożliwia tworzenie grup urządzeń, 19. Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania

	m.in. magazynów). 20. System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: a. System Administrator, b. Backup operator, c. Restore operator, d. Viewer.

Składowanie danych:	1. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie z poziomu jednej konsoli, 2. System umożliwia składowanie danych: a. Lokalnie: ■ Zasób SMB, ■ Zasób NFS, ■ Zasób ISCSI, ■ Zasób S3, ■ Katalog zabezpieczonego urządzenia. b. W chmurze: ■ Amazon Web Service, ■ Magazyn zgodny z S3, ■ Dostarczanej bezpośrednio przez producenta. 3. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, 4. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
Odtwarzanie:	1. Odtwarzanie granularne: a. Pojedynczych plików z kopii obrazu dysku, b. Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, 2. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: a. Windows: 7+, b. Windows Server: 2008 R2+, 3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 4. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a, 5. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. 6. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK), 7. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), 8. Odtwarzanie zasobów plikowych z prawami dostępu, 9. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), 10. Odtwarzanie danych według harmonogramu, 11. Przywracanie danych z określonego urządzenia/użytkownika, 12. Przywracanie kopii z wybranego magazynu.

	13. Przywracanie danych Microsoft 365: a. do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku: ■ pst, ■ mbox. b. do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), 14. System posiada możliwość nieodwracalnego kasowania danych, 15. Przywracanie repozytoriów GIT: a. Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket), b. przywracanie między kontami.

Backup:	1. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: a. Systemów operacyjnych: ■ Alpine 3.10+, ■ Debian: 9+, ■ Ubuntu: 16.04+, ■ Fedora: 29+, ■ centOS: 7+, ■ RHEL: 6+, ■ openSUSE: 15+, ■ SUSE Enterprise Linux(SLES): 12 SP2+, ■ macOS: 10.13+, ■ Windows: 7, 8.1, 10(1607+), ■ Windows Server: 2008 R2+, b. Środowisk wirtualnych: ■ Hyper-V, ■ VMware: 6.7+. ■ Dowolne inne w sposób agentowy c. Repozytoriów GIT: ■ GitHub, ■ Bitbucket. 2. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla: **a.** Baz danych**:** ■ Microsoft SQL, ■ MySQL, ■ PostgreSQL, ■ Firebird, ■ Dowolnych innych przez podpięcie skryptów pre/post. 3. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: a. 128 bit, b. 192 bit, c. 256 bit. 4. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: a. ZStandard, b. LZ4. 5. Oprogramowanie umożliwia zarządzanie poziomem kompresji, 6. Wykonywanie kopii zapasowej otwartych plików(VSS), 7. System umożliwia uruchamianie skryptów przed i po backupie, 8. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, 9. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, 10. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,

	11. Backup plikowy, 12. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, 13. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, 14. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, 15. Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. 16. Oprogramowanie pozwala na backup zaszyfrowanych partycji.
GIT	1. Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), 2. Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).
Licencjonowanie:	Sposób licencjonowania opiera się na: • Ilości serwerów/endpointów- dla fizycznych urządzeń, • Ilości gniazd na procesor na hoście fizycznym - dla środowisk wirtualnych, • Ilości repozytoriów - dla GIT, • ilości użytkowników dla ekosystemu Microsoft Office 365. Licencje w wersji wieczystej : • licencje per gniazdo procesora. ● Wsparcie techniczne: o Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta, o Zapewnia dostęp do aktualizacji oprogramowania, o Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, **o Obowiązuje przez okres minimum 36 miesięcy.**

Wdrożenie:	• Dopuszczone wdrożenie w formie zdalnej, • W procesie wdrożenia musi być zapewnione wsparcie producenta oprogramowania, • Wdrożenie musi się odbyć w języku polskim, • Wdrożenie musi obejmować krótkie, podstawowe szkolenie z obsługi oprogramowania.

6.4. Serwer NAS typ 1 – 1 szt.

Parametr	Minimalne wymagania
Typ	Sieciowy serwer plików NAS
Zastosowanie	Serwer kopii zapasowych. Praca ciągła (24/7/365)
Architektura procesora	64-bit x86
Procesor liczba rdzeni	Nie mniej niż 6
Częstotliwość taktowania	Minimum 3.6 GHz
Pamięć RAM	Nie mniej niż 8GB DDR4
Pamięć RAM liczba slotów	Minimum 4 sloty
Pamięć RAM - możliwość rozszerzenia	nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski twarde	Minimum 8
Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA / SSD SATA
Pojemność dysków twardych jakie można stosować	do 18 TB
Zainstalowane dyski	4 szt. min. 6TB 3,5'' 256MB SATAIII/7200rpm, dyski klasy Enterprise NAS
Możliwość podłączenia modułu rozszerzającego	Urządzenie powinno wspierać rozbudowę o minimum 9 modułów rozszerzających, dostarczenie modułów, kart rozszerzeń lub przewodów nie jest wymagane
Porty LAN	Minimum 2 x 1 Gb/s Ethernet oraz 2 x 10 Gb/s SFP+
Diody LED	HDD 1–8, stan, LAN, stan gniazda rozszerzenia pamięci masowej
Porty USB 3.2 Gen1	Min. 4
Porty USB 3.2 Gen 2 (10 Gb/s)	Min. 1 x typ C min. 1 x typ A
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U, szyny do montażu w szafie rack
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Redundantne 2 x min. 300 W , 100–240 V
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+

Możliwość podłączenia karty WLAN na USB	Tak
Łączenie usług z interfejsem	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, RAID 0, 1, 5, 50, 6, 60, 10, 5+Hot Spare, 6+Hot Spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Globalny Hot Spare, Pula pamięci masowej Mechanizm automatycznego pozycjonowania danych w zależności od częstotliwości wykorzystania SSD over provisioning Funkcjonalność migawek dla woluminów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie Obsługa SSD cache w trybach read i write
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii plików dla systemów Windows producenta urządzenia Serwer Apple Time Machine Backup na zewnętrzne dyski twarde

Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox,
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer baz danych MySQL Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu (opcja podłączenia 8 kamer IP w ramach wbudowanych licencji z możliwością podłączenia dodatkowych po dokupieniu licencji)
VPN	VPN client / VPN server Obsługa PPTP Obsługa OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania ręczna Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia: Kopi zapasowej ustawień, przywracania, resetowania systemu

Wirtualizacja	Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android; import maszyn wirtualnych z systemów VirtualBox, Vmware Workstation; VM clone, VM snapshot; pass-through dla USB;
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem adresów Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek oraz wbudowane narzędzia wirtualizacji umożliwiające zarówno obsługę kontenerów Docker/LXD jak i pełnych maszyn wirtualnych
Gwarancja	Producenta min. 12 miesięcy, uszkodzone dyski pozostają u klienta

6.5 Serwer NAS typ 2 – 1 szt.

Parametr	**Minimalne wymagania**
Typ	Sieciowy serwer plików NAS
Zastosowanie	Serwer kopii zapasowych, przechowywawnie i współdzielenie plików. Praca ciągła (24/7/365)
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 4 zatoki 3,5"
Obsugiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD
Wbudowane w urządzenie interfejsy na dyski M2	Wymagane min. 2 x M2 PCIe Gen3x1
Możliwość stosowania dysków twardych o pojemności	do 18TB
Zainstalowane dyski	Min. 4 szt. min. 4TB 3,5'' 256MB SATAIII/7200rpm, dyski klasy Enterprise NAS

Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 3
Port PCiE	Tak, minimum 2 Gen3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL

Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie

Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	Min. 12 miesięcy, uszkodzone dyski pozostają u klienta

6.6 Serwer NAS typ 3 – 1 szt.

Parametr	**Minimalne wymagania**
Typ	Sieciowy serwer plików NAS
Zastosowanie	Serwer kopii zapasowych, przechowywanie i współdzielenie plików. Praca ciągła (24/7/365)
Procesor	Min. 4-rdzeniowy/ min. 4-wątkowy procesor o taktowaniu zwiększanym do 2,9 GHz
Architektura procesora	64-bitowy x86
Procesory graficzne	Intel UHD Graphics lub równoważny
Koprocesor arytmetyczny FPU	TAK
Mechanizm szyfrowania	(AES-NI)
Transkodowanie wspomagane sprzętowo	TAK
Pamięć systemowa	Min. 8 GB RAM
Pamięć flash	Min. 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem)
Wnęka dysków	Min. 2 dysków 3,5-calowych SATA 6 Gb/s
Zainstalowane dyski	2 szt., min. 8TB 3,5” 256MB/5640RPM, dyski klasy NAS
Kompatybilność dysków	3.5-inch SATA hard disk drives 2.5-inch SATA solid state drives
Wymieniany podczas pracy	TAK
Gniazdo M.2	Min. 2 x M.2 2280 PCIe Gen 3 x1
Obsługa przyspieszenia pamięci podręcznej SSD	TAK
Port 2,5 Gigabit Ethernet	Min. 2

(2,5G/1G/100M/10M)	
Wake on LAN (WOL)	TAK
Ramka Jumbo	TAK
Gniazdo PCIe	Min. 1 Gniazdo 1: PCIe Gen 3 x2
Port USB 2.0	Min. 2
Port USB 3.2 Gen 2 (10 Gb/s)	Min. 2 x typu A
Czujnik podczerwieni	Opcjonalny pilot
Wyjście HDMI	Min. 1, HDMI 2.1
Kształt	Tower
Wskaźniki LED	Zasilanie/stan, LAN, USB, HDD1–2
Przyciski	Zasilanie, kopiowanie USB, reset
Wentylator	TAK
Ostrzeżenie systemowe	Brzęczyk
Gniazdo bezpieczeństwa Kensington	TAK
Maks. liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci	Min. 1500
Obsługiwane 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. Microsoft Windows 7, 8, 10 and 11 4. Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, and 2019
Obsługiwane przeglądarki	1. Apple Safari 2. Google Chrome 3. Microsoft Edge 4. Mozilla Firefox
Obsługiwane języki	Min. polski, angielski
Maksymalny rozmiar wolumenu	250 TB
Liczba obsługiwanych udziałów	Min. 512
JBOD Expansion	Tak
iSCSI Service	TAK
Obsługiwane poziomy RAID	JBOD, Single, RAID 0, 1
RAID Level Migration	TAK
RAID Expansion (by adding Disk)	TAK
System plików	EXT4
File Server	1. File sharing across Windows, Mac, and Linux/UNIX 2. Microsoft networking (CIFS/SMB) 3. Apple networking (AFP) 4. NFS version 3/4 services
FTP Server	1. QuFTP 2. FTP, SFTP and TFTP protocols 3. FTP over SSL/TLS (explicit FTPS) 4. FXP support
Maksymalna liczba połączeń FTP	1024
Liczba użytkowników lokalnych	Min. 4,096
Liczba grup lokalnych	Min. 512

Gwarancja	Producenta min. 12 miesięcy, uszkodzone dyski pozostają u klienta

6.7 System bezpieczeństwa sieciowego – szt. 1

Parametr	**Minimalne wymagania**
Typ	Firewall sprzętowy UTM

Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

	3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.

Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych

	repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w

	nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
Gwarancja oraz wsparcie	1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Opisy do wymagań ogólnych	1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

6.8 Monitor interaktywny wraz z montażem – 4 szt.

Parametry	Minimalne wymagania
Charakterystyka wyświetlacza	Matryca z podświetleniem LED o żywotności min. 50 000 godzin. Szyba matowa, antyodblaskowa, wzmacniana, hartowane szkło min. 4mm o

	twardości 7H w skali Mohsa
Przekątna ekranu	Min. 65"
Kontrast statyczny	Min. 5000:1
Kontrast dynamiczny	Min. 6000:1
Jasność typowa	Min. 450cd/m2
Czas reakcji	Min . 8ms
Kąt widzenia typowy	Min. 178◦ w poziomie i pionie
Rozdzielczość podstawowa	Min. 3840*2160 Pixel (4K) przy 60Hz
Pamięć wbudowania	Min. 2GB RAM Min. 16GB ROM
Wymagania dodatkowe	Min. 3x wejścia HDMI, Min. 1x VGA, Min. 1x PC AUDIO, Min. 1x port OPS Min. 6x wejścia USB w tym min. 3x USB 2.0 i min. 3x USB 3.0, Min. 2x Dotyk, Min. 1x TF Card (wsparcie dla kart do 64GB), Min. 1x RS232, Min. 1x LAN (RJ45) Min. 1x karta sieciowa WIFI Min. 1x USB-A – interfejs komunikacyjny Wbudowane min. 2x głośniki stereo o mocy min. 16W Technologia Zero Gap lub równoważne Liczba punktów dotykowych: min. 20(dotyk), min. 10(pisanie) Metoda obsługi: min Długopis (>3mm szerokości) lub palec
Wymiary obszaru wyświetlania (szerokość*wysokość)	Min. 1428x 803 mm
System	Dedykowany przez producenta
Wyjścia	Min. 1x wyjście HDMI (4K2K), Min. 1x wyjście Audio, Min. 1x COAX Out
Gwarancja	Min. 1 rok producenta
Certyfikaty	Zgodność z dyrektywą ROhs, Certyfikat CE
Akcesoria i wyposażenie	1x Kabel zasilający 230V, 1 x kabel HDMI (min. 3M), 1x Kabel USB (min. 5M) 1x Pilot, min. 2x pisaki 1x uchwyt ścienny o nośności max. 55kg, odległość od ściany max. 25mm, regulacja konta pochylenia min. 0 stopni – max. 14 stopni, VESA 600x400mm

Szczegóły dot. montażu	Montaż należy wykonać w następującej kolejności: 1) dostawa monitora do siedziby wskazanej przez Zamawiającego (SP Obrubniki) wraz z niezbędnym wyposażeniem, 2) montaż naściennego uchwytu we wskazanym przez pracowników Zamawiającego miejscu, zawieszenie monitora, uruchomienie.

6.9 Notebook typ 1- 16 szt. Wymagania minimalne

Parametry	**Wymagania minimalne**
Typ	Komputer przenośny typu Notebook
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do internetu oraz poczty elektronicznej
System operacyjny	Windows 11 Pro wersja Education, PL lub równoważny*
Procesor	Procesor wielordzeniowy, uzyskujący wynik co najmniej 6180 punktów w teście Passmark – CPU Mark wg wyników procesorów publikowanych na stronie https://www.cpubenchmark.net/cpu_list.php najpóźniej w dniu złożenia oferty
Karta graficzna	Min. Zintegrowana karta graficzna
Ekran	Min. 15,6-calowy, FHD (1920 x 1080)
Pamięć	Minimum 8GB DDR4
Dyski	Dysk SSD z interfejsem M.2 NVMe PCIe min. 3.0 minimum 256 GB
Interfejsy	Min. 1 x USB 3.2 Gen 1 Type-A Min. 1 x USB 3.2 Gen 1 Type-C Min. 2 x USB 2.0 Type-A Min. x HDMI 1.4 Min. 1 x gniazdo audio mini-jack 3,5 mm typu combo Min. 1 x wejście zasilania DC
Gniazda rozszerzeń	Min. 1 x gniazdo DDR4 SO-DIMM min. 1 x M.2 2280 PCIe 3.0 x4 min. 1 x HDD 2,5” SATA STD
Kamera internetowa	Wbudowana min. 720p HD
Dźwięk	Zintegrowany głośnik Zintegrowany mikrofon
Łączność bezprzewodowa	Min. Wi-Fi 5(802.11ac) Bluetooth min. 5.1
Bateria	Min. 37 WHr
Zasilanie	Zewnętrzny zasilacz sieciowy 230V od producenta komputera przenośnego wraz z kablami przejściowymi
Certyfikaty i standardy	Standard Energy star min. 8.0, spełniający normy MIL-STD-810H (załączyć oświadczenie producenta do oferty) lub przechodzący pozytywnie wszystkie testy kwalifikujące do otrzymania standardu MIL-STD-810H. min.
Producent sprzętu	Wszystkie sztuki muszą pochodzić od jednego producenta
Gwarancja	Producenta min. 12 miesięcy ONSITE

Opis równoważności dla systemu MS Windows 11 PRO wersja Edukacyjna
*równoważne tj. spełniające poniższe warunki:
1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika,
2. System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016, 2019; MS Visio 2007, 2010, 2016; MS Project 2007, 2010, 2016.
3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
4. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,

5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
6. Wbudowany system pomocy w języku polskim,
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
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. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: i. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
21. Obsługa standardu NFC (near field communication),
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
24. 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),
25. Mechanizmy wieloelementowego uwierzytelniania.
26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
27. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
29. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
30. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
31. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
32. 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,
33. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
34. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,

35. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
36. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
37. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
38. 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.),
39. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
40. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
42. 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.
43. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
44. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
45. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

6.10 Notebook typ 2- 3 szt.

Wymagania minimalne

Parametry	Wymagania minimalne
Typ	Komputer przenośny typu Notebook
	Do zadań biurowych, praca z programami graficznymi, aplikacjami biurowymi, dostęp do internetu oraz poczty elektronicznej
System operacyjny	Windows 11 Pro lub równoważny*
Procesor	Procesor wielordzeniowy, uzyskujący wynik co najmniej 6180 punktów w teście Passmark – CPU Mark wg wyników procesorów publikowanych na stronie https://www.cpubenchmark.net/cpu_list.php
Karta graficzna	Min. Zintegrowana karta graficzna
Ekran	Min. 15,6-calowy, FHD (1920 x 1080)
Pamięć	Minimum 8GB DDR4
Dyski	Dysk SSD z interfejsem M.2 NVMe PCIe min. 3.0 minimum 256 GB
Interfejsy	Min. 1 x USB 3.2 Gen 1 Type-A Min. 1 x USB 3.2 Gen 1 Type-C Min. 2 x USB 2.0 Type-A Min. 1 x HDMI 1.4 Min. 1 x gniazdo audio mini-jack 3,5 mm typu combo Min. 1 x wejście zasilania DC
Gniazda rozszerzeń	Min. 1 x gniazdo DDR4 SO-DIMM Min. 1 x M.2 2280 PCIe 3.0 x4 Min. 1 x HDD 2,5” SATA STD
Kamera internetowa	Wbudowana min. 720p HD
Dźwięk	Zintegrowany głośnik Zintegrowany mikrofon
Łączność bezprzewodowa	Min. Wi-Fi 5(802.11ac) Bluetooth min. 5.1

Bateria	Min. 37 WHr
Certyfikaty i standardy	Standard Energy star min. 8.0, spełniający normy MIL-STD-810H (załączyć oświadczenie producenta do oferty) lub przechodzący pozytywnie wszystkie testy kwalifikujące do otrzymania standardu MIL-STD-810H. min.
Producent sprzętu	Wszystkie sztuki muszą pochodzić od jednego producenta
Gwarancja	Producenta min. 12 miesięcy ONSITE

Opis równoważności dla systemu MS Windows 11 PRO

*równoważne tj. spełniające poniższe warunki:

1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika,

2. System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016, 2019; MS Visio 2007, 2010, 2016; MS Project 2007, 2010, 2016.

3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:

a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

4. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,

5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,

6. Wbudowany system pomocy w języku polskim,

7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,

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. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: i. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,

20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.

21. Obsługa standardu NFC (near field communication),

22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);

23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;

24. 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),

25. Mechanizmy wieloelementowego uwierzytelniania.

26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,

27. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,

28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;

29. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,

30. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,

31. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,

32. 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,

33. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,

34. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,

35. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.

36. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,

37. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,

38. 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.),

39. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),

40. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,

41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,

42. 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.

43. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych

44. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

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

6.11 Oprogramowanie antywirusowe- pakiet edukacyjny – 50 licencji

Parametry	Wymagania ogólne
Opis ogólny	Oprogramowanie antywirusowe Pakiet Edukacyjny dla 50 stanowisk min. 12 miesięcy
	Centralne zarządzanie z poziomu jednej konsoli, która zapewnia wgląd we wszystkie komponenty zarządzania bezpieczeństwem. Umożliwia automatyczne tworzenie w czasie rzeczywistym kopii zapasowych plików przed atakiem ransomware Zapobiega i blokuje na etapie wykonania w punktach końcowych oraz siec Monitoruje działania procesów w czasie rzeczywistym oraz automatyczne/ręczne zakończenie w razie podejrzanej lub złośliwej aktywności Eliminuje podatność na ataki ransomware powodowane lukami w systemach i aplikacjach, błędami konfiguracji lub ryzykownymi działaniami użytkowników.
Obszar zastosowań	akademicki

Kamera internetowa- 3 szt.

Wymagania minimalne

Parametr	Wymagania minimalne
Typ	Kamera internetowa
Zastosowanie	Wideo konferencje, webinaria
Mikrofon	Wielokierunkowy zintegrowany podwójny cyfrowy mikrofon MEMS
Interfejs	min. USB 2.0 Zgodne z Plug and Play UVC (klasa urządzeń wideo USB) Długość przewodu: min. 1,8 m min. 1x Złącze USB-A Montaż na statywie: tak
Przetwarzanie obrazu	Technologia matrycy: CMOS Matryca min. Full HD (1920 × 1080) min. 2 Mpx Rozdzielczość wideo: MJPG – 1080p min. 30 kl./s / 720p min. 30 kl./s YUY2 - 1080p min. 5 kl./s , 720p min. 10 kl./s Format wyjściowy: min. YUY2 / MJPG Liczba klatek na sekundę: do 30 kl./s przy rozdz. 1080p Rozdzielczość przechwytywania obrazu: min. 1920 × 1080 / min. 1280 × 720 Format zapisywanego obrazu: min. BMP/JPG Pole widzenia: min. 77° po przekątnej Zasięg zbierania dźwięku: min. 500 mm / 50 cm do nieskończoności. Optymalny zasięg: min. 600 mm / 60 cm Kamera internetowa wyposażona w zintegrowaną osłonę obiektywu Obrót w poziomie o min. 360 ° i pochylenie w pionie o min. 30 ° Uniwersalny klips montażowy, z możliwością przymocowanie do statywu
Gwarancja	Min. 12 miesięcy lata producenta

Słuchawki- 2 szt.

Wymagania minimalne

Parametr	Wymagania minimalne
Typ	Słuchawki
Zastosowanie	Wideokonferencje, obróbka audio wideo
typ słuchawek	zamknięte, dynamiczne
przetwornik akustyczny	Min. 40 mm
impedancja	Min. 48 omów (połączenie przewodem słuchawkowym, urządzenie włączone), Min. 16 omów (połączenie przewodem słuchawkowym, urządzenie wyłączone)
pasmo przenoszenia	Min. 7 – mx. 25 000 hz (jeita)
pasmo przenoszenia (komunikacja bluetooth)	20–20 000 hz (próbkowanie 44,1 khz) / 20–40 000 hz (ldac, próbkowanie 96 khz, 990 kb/s)
czułości (db/mw)	96 db/mw (połączenie przewodem słuchawkowym, urządzenie włączone), 96 db/mw (połączenie przewodem słuchawkowym, urządzenie wyłączone)
regulacja głośności	czujnik dotykowy
typ przewodu	jednostronny (odłączany)
długość przewodu	Min. 1 m
wejścia	Min. 1x mini jack stereo
praca w trybie pasywnym	tak
czas pracy akumulatora (ciągłe odtwarzanie muzyki)	maks. 30 godzin (z włączoną redukcją hałasu) / maks. 50 godzin (z wyłączoną redukcją hałasu)
czas pracy akumulatora (ciągła komunikacja)	maks. 30 godzin (z włączoną redukcją hałasu) / maks. 40 godzin (z wyłączoną redukcją hałasu)
bluetooth	Wersja min. 5.2
efektywny zasięg	Min. 10 m
zakres częstotliwości	pasmo 2,4 Ghz (2,4000 – 2,4835 Ghz)
Standard bezprzewodowego przesyłania dźwięku	a2dp, avrcp, hfp, hsp
obsługiwane formaty audio	sbc, aac, ldac
obsługiwane systemy ochrony treści	Kompatybilne z scms-t
wyłącznik systemu redukcji hałasów	tak
Dodatkowe akcesoria	• torba • przewód połączeniowy • przewód usb type-c
Gwarancja	Min. 12 miesięcy producenta

Dysk przenośny zewnętrzny- 2 szt.

Wymagania minimalne

Parametr	Wymagania minimalne
Typ	Dysk przenośny zewnętrzny
Zastosowanie	Przenoszenie plików
Rodzaj dysku	zewnętrzny
Typ	HDD (magnetyczny)
Format	2.5 cala
Interfejs	Min. USB 3.2 Gen 1

Pojemność	Min. 2000 GB
Gwarancja	Min. 12 miesięcy producenta

Pamięć przenośna Pendrive – 3 szt.

Wymagania minimalne

Parametr	Wymagania minimalne
Typ	Pamięć przenośna typu pendrive
Zastosowanie	Przenoszenie plików
Pojemność	Min. 64GB
Szybkość	USB min 3.2 gen 1
Gwarancja producenta	Min. 12 miesięcy