Załącznik nr 1
Szczegółowy opis przedmiotu zamówienia

Sierpień 2022

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.
   - całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
   - całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;
   - całość sprzętu nie może mieść zaległości/obciążenia, zobowiązań itd. oraz nie może być zakupiona ze środków pomocowych

2. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. 12 miesięczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparte na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca musi udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

Oprogramowanie

- oprogramowanie powinno posiadać min.12-miesięczną gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

3. Miejsce instalacji sprzętu i oprogramowania/systemu.
   - Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika nr 1, w budynku Urzędu Gminy Iłów pod adresem: ul. Płocka 2 , 96-520 Iłów miejscach wskazanych przez Zamawiającego.

1. Minimalne wymagania techniczne dla przedmiotu zamówienia – Komputer typ All-in-One PC Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do Internetu oraz poczty elektronicznej

Asortyment	Parametr	Wartość minimalna
1.	2.	3.
Komputer stacjonarny typu All in One. W ofercie wymagane jest podanie modelu, symbolu oraz producenta		
	Procesor	Min. *6*-rdzeniowy, min *3.00GHz*, ***z technologią vPro***, osiągający w zaoferowanej konfiguracji w teście PassMark CPU Mark wynik min. **20000** punktów. Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów SIWZ
	Pamięć operacyjna	*1 x 8GB* 4800 MHz DDR5 możliwość rozbudowy do min 64GB, minimum *jeden* slot wolny na dalszą rozbudowę
	Parametry pamięci masowej	Min. *256 GB M.2 PCIe NVMe*
	Grafika	Zintegrowana z procesorem, ze wsparciem dla DirectX 12, OpenGL 4.5 oraz dla rozdzielczości 4096x2160@60Hz osiągająca w teście Average G3D Mark wynik na poziomie 2600 punktów. Do oferty należy dołączyć wydruk ze strony: http://www.videocardbenchmark.net potwierdzający spełnienie wymogów SIWZ

	Wyposażenie multimedialne	karta dźwiękowa zintegrowana z płytą główną; wbudowane dwa głośniki stereo o mocy 5W na kanał.
	Obudowa	Obudowa typu All in One – zintegrowany komputer w obudowie wraz z monitorem z matrycą IPS min 23,8” o parametrach: - rozdzielczośc min 1920 x 1080 @ 60 Hz - kontrast typowy min 1000:1, - plamka max 0,275 - typowa jasność min 250 cd/m2, matryca matowa bez dotyku - kąty widzenia pion/poziom: min 178/178 stopni - kąty pochylenia w pionie min -5/+18 stopni Dodatkowo dla standu Adjustable Height: - regulacja wysokości do 130 mm - Swivel +/- 45 stopni Waga max 7 kg bez standu Waga max 9,4 kg ze standem Adjustable Height Wymiary bez standu: 54 x 5,3 x 39 cm Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta. Wymagany jest wbudowany fabrycznie dźwiękowo-wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej: – awarie procesora – uszkodzenie kontrolera Video – uszkodzenie pamięci RAM Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) Zasilacz wewnętrzny o mocy max: 280W o sprawności min 89% Komputer musi być wyposażony w menu ekranowe z poziomu którego użytkownik może ustawić jasność, kontrast oraz włączyć technologie obniżającą poziom niebieskiego światła (tzw Low Blue Light) oraz tryb nocny (tzw Night Light).
	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z wymaganym systemem operacyjnym
	BIOS	Możliwość odczytania z BIOS: 1. Wersji BIOS wraz z datą wydania wersji 2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3 3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych

		slotach 4. Informacji o dysku twardym: model, pojemność, 5. Informacji o napędzie optycznym: model, 6. Informacji o MAC adresie karty sieciowej Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, serial portu, portów USB (bok, tył), funkcjonalności ładowania zewnętrznych urzadzeń przez port USB, poszczególnych slotów SATA, czytnika kart SD, audio, funkcji TurboBoost, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Diagnostyka uruchamiana z BIOS działająca bez obecności systemu operacyjnego czy dysku twardego umożliwiająca na przeprowadzenie testów diagnostycznych w tym m.in.: - test procesora - test dysku twardego - test pamięci RAM - test płyty głównej
	Bezpieczeństwo	1. BIOS musi posiadać możliwość - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, - możliwość ustawienia hasła na dysku (drive lock) - blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; - kontroli sekwencji boot-ącej; - startu systemu z urządzenia USB - funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń 2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0); 3. Możliwość zapięcia linki typu Kensington i kłódki do dedykowanego oczka w obudowie komputera 4. Czujnik otwarcia obudowy zintegrowany trwale z płytą główną i zarządzany z poziomu BIOS w zakresie min włączyć/wyłączyć. 5. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez

		konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funcjonalności systemu diagnostycznego: - informacje o systemie, min.: 1. Procesor: typ procesora, jego obecną prędkość 2. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamieci, nr seryjny, typ pamieci, nr częsci, nazwa producenta 3. Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku 4. Napęd optyczny: model, wersja firmware, nr seryjny 5. Data wydania i wersja BIOS 6. Nr seryjny komputera - możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera - możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiekowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej - rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
	Certyfikaty i standardy	– Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) – Deklaracja zgodności CE (załączyć do oferty) – Komputer musi spełniać wymogi normy Energy Star Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej - Komputer musi spełniać wymogi dla TCO 8.0 i TCO Edge – dopuszcza się wydruk ze strony https://tcocertified.com/
	Ergonomia-	Maksymalnie 15,4 dB z pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; Do oferty należy dołączyć oświadczenie producenta o spełnianiu ww. wymogów/
	Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Do oferty należy dołączyć oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
	Wsparcie techniczne producenta	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: - weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć) - czasu obowiązywania i typ udzielonej gwarancji Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych

		wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera
	Wymagania dodatkowe	1. Wbudowane porty i złącza: - porty wideo: min. 1 szt DisplayPort 1.4 (DP++), HDMI-in 1.4 - min. 7 x USB w tym min: 1 szt USB 3.2 Gen 2 Typ-C o przepustowości do 20 Gbps z boku obudowy, 1 szt USB 3.2 Gen 2 Typ-C o przepustowości do 10 Gbps z tyłu obudowy, 1 szt USB 3.2 Gen 2 Typ-A o przepustowości do 10 Gbps z boku obudowy, 2 szt USB 3.2 Gen 1 Typ-A o przepustowości do 10Gbps z tyłu obudowy, 2 szt USB 3.2 Gen 1 Typ-A o przepustowości do 5Gbps z tyłu obudowy - port sieciowy RJ-45 - port audio COMBO *kamera internetowa:* *- 5 MP RGB webcam z dwoma mikrofonami i diodą doświetlającą; max rozdzielczość 2592 x 1944* Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp. 2. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL, *vPro* 3. Karta WiFi *Intel AX211 Wi-Fi 6E vPro 160 MHz +Bluetooth 5.3 z vPro* 4. Płyta główna z chipsetem min Q670, wyposażona w: - 2 złącza SODIMM z obsługą do 64GB pamięci RAM 4800 MHz DDR5 - 1 złącze M.2 PCIe x1 dla WLAN - 3 złącze M.2 PCIe x4 dla dysku SSD 5. Klawiatura USB w układzie polski programisty 6. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll)
	Zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, posiadająca sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiająca: - monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS płyty głównej; - zdalną konfigurację ustawień BIOS; - zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; - zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; - technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0

		(http://www.dmtf.org/standards/mgmt/dash/); - nawiązywanie przez sprzętowy mechanizm zarządzania zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; - wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego. - zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie

2. Minimalne wymagania techniczne dla przedmiotu zamówienia – Komputer przenośny typ notebook

Asortyment	**Parametr**	**Wartość minimalna**
1.	2.	3.
Komputer przenośny	Typ	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości: FHD (1920x1080) w technologii LED IPS przeciwodblaskowy, jasność min 250 nitów, kontrast min 600:1, kąty widzenia góra/dół/lewo/prawo: 85/85/85/85. Komputer przenośny typu notebook z ekranem dotykowym 15,6" o rozdzielczości: FHD (1920x1080) w technologii LED IPS przeciwodblaskowy, jasność min 250 nitów, kontrast min 600:1, kąty widzenia góra/dół/lewo/prawo: 85/85/85/85.
	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
	Procesor	Procesor klasy x86, **10** rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej **1,7** GHz, z pamięcią last level cache CPU co najmniej **12** MB lub równoważny **4** rdzeniowy procesor klasy x86 Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik min.: **13 500** punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net) – wydruk ze strony należy dołączyć do oferty. W przypadku użycia przez oferenta testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności

		przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
	Pamięć operacyjna RAM	**16 GB DDR4,** możliwość rozbudowy do min 32GB
	Parametry pamięci masowej	**Min. 512 GB SSD M.2 NVMe**
	Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12.1, OpenGL 4.6, Osiągająca w teście Average G3D Mark wynik na poziomie min.: **2750** punktów (wynik zaproponowanej grafiki musi znajdować się na stronie http://www.videocardbenchmark.net) – wydruk ze strony należy dołączyć do oferty.
	Wyposażenie multimedialne	Karta dźwiękowa stereo, wbudowane dwa głośniki stereo 2W/4 omy dla każdego z głośników Wbudowana w obudowę matrycy kamera HD 720p @ 30 fps wraz z mikrofonem
	Wymagania dotyczące baterii i zasilania	3-cell, 51WHr, Li-Ion, Long-Life. Czas pracy na baterii wg dokumentacji producenta min 12,5 godziny Funkcja szybkiego ładowania baterii umożliwiająca naładowanie baterii do 50% jej pojemności w czasie 30 min (+/-10%) (wymagany jest wtedy zasilacz o mocy min 45W) Zasilacz o mocy min. **65 W**
	Certyfikaty i standardy	– Certyfikat ISO 9001:2000 dla producenta sprzętu (należy załączyć do oferty) – Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) – Deklaracja zgodności CE (załączyć do oferty) – Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy załączyć do oferty) – Wydruk ze strony WHCL Microsoft potwierdzający zgodność oferowanego komputera z oferowanym system operacyjnym lub oświadczenie producenta. – (należy załączyć do oferty) – Certyfikat EPEAT 2019 na poziomie GOLD dla Polski. Wymagany wpis dotyczący oferowanej stacji dostępowej w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej I – Certyfikat EnergyStar 8.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov Certyfikat TCO – wymagany wpis dla modelu na stronie TCO https://tcocertified.com/
	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie (IDLE) wynosząca maksymalnie 15,4dB (wartość do zweryfikowania w dokumentacji technicznej komputera oraz należy załączyć oświadczenie producenta). (należy załączyć do oferty)

	Waga i wymiary	Waga 1.79 Kg z baterią 3-cell Szerokość: max 35,94 mm Głębokość: max 234 mm Wysokość: max 19,9 mm
	BIOS	Możliwość odczytania z BIOS: 1. Wersji BIOS wraz z datą wydania wersji 2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3 3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach 4. Informacji o dysku twardym: model 5. Informacji o MAC adresie karty sieciowej 6. Zaimplementowany w BIOS podstawowy system diagnostyczny umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego: - test procesora - test pamięci RAM - test dysku twardego - test baterii - test płyty głównej Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, portów USB, funkcjonalności ładowania zewnętrznych urządzeń przez port USB, wewnętrznych głośników, funkcji TurboBoost, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła dla BIOS na poziomie administratora. Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła dla dysku twardego w tym również dla dysków NVMe. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. W BIOS musi być zaimplementowany mechanizm trwałego kasowania danych z dysków twardych zainstalowanych w komputerze w tym również dysków SSD NVMe – mechanizm uruchamiany na życzenie przez użytkownika.
	Bezpieczeństwo	1. BIOS musi posiadać następujące cechy: - możliwość autoryzacji przy starcie komputera każdego użytkownika jego hasłem indywidualnym lub hasłem administratora -kontrola sekwencji bootującej;

		- możliwość startu systemu z urządzenia USB - funkcja blokowania Bootowania stacji roboczej z zewnętrznych urządzeń - BIOS musi zawierać nieulotną informację z nazwą produktu, jego numerem seryjnym, wersją BIOS, zainstalowanym fabrycznie systemem operacyjnym, a także informację o: typie zainstalowanego procesora, ilości pamięci RAM, 2. Możliwość zapięcia linki typu Kensington 3. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0) 4. Obudowa o wzmocnionej konstrukcji, spełniająca wymogi normy Mil-Std-810H w zakresie min 19 testów (załączyć oświadczenie producenta). 5. Zaimplementowany w BIOS mechanizm zakładania hasła dla dysków twardych zainstalowanych w komputerze w tym również dla dysków SSD NVMe. 6. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. System diagnostyczny może być zainstalowany na ukrytej dedykowanej partycji dysku twardego. Minimalne funkcjonalności systemu diagnostycznego: - informacje o systemie, min.: 1. Procesor: typ procesora, jego obecna prędkość 2. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta 3. Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku 4. Napęd optyczny: model, wersja firmware, nr seryjny 5. Data wydania i wersja BIOS 6. Nr seryjny komputera - możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera - możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej - rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii Komputer musi być wyposażony w zintegrowany z płytą główną szyfrowany kontroler fizycznie odizolowany, odpowiedzialny za weryfikację i ochronę BIOS oraz jego samoczynną naprawę w przypadku nieautoryzowanego jego nadpisania lub uszkodzenia. Komputer musi być wyposażony w BIOS posiadający mechanizm samokontroli i samoczynnej autonaprawy, działający automatycznie przy każdym uruchomieniu komputera, który sprawdza integralność i autentyczność uruchamianego podsystemu BIOS oraz musi chronić Master Boot Record (MBR) oraz GUID Partition Table (GPT) przed uszkodzeniem lub usunięciem. Weryfikacja poprawności BIOS musi się odbywać z wykorzystaniem zintegrowanego z płytą główną szyfrowanego kontrolera fizycznie odizolowanego o którym mowa w wyżej. Mechaniczna przesłona kamery zintegrowana w ramce matryc.

	Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzonego przez Producenta, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta
	Wymagania dodatkowe	1. Wbudowane porty i złącza: 1 x HDMI 1.4b, 3 szt. USB typ-A 3.2 Gen 1 w tym 1 szt z ładowaniem zewnętrznych urządzeń, 1 szt USB 3.2 Gen 2 typu-C, RJ-45, 1 x złącze słuchawkowe stereo/mikrofonowe (combo audio), czytnik kart multimedialnych micro SD, wbudowana kamera 720p@30fps w obudowę ekranu komputera i dwa mikrofony 2. Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną oraz WLAN-**AX** 802.**11a/b/g/n/ac/ax wraz z Bluetooth 5.2 COMBO**, zintegrowany z płytą główną lub w postaci wewnętrznego modułu mini-PCI Express. 3. Klawiatura (układ US -QWERTY) odporna na zalanie, 4. Touchpad/Clickpad 5. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. 6. Kąt otwarcia ekranu notebooka min 180 stopni. 7. Obudowa zewnętrzna matrycy oraz wokół klawiszy wykonana z aluminium.
	System Operacyjny	(Proszę podać jeżeli sprzęt posiada system operacyjny) Wymagany w wersji Pro

3. Minimalne wymagania techniczne dla przedmiotu zamówienia – Przełącznik sieciowy.

Asortyment	Parametr	Wartość minimalna
1.	2.	3.
Switch	**Parametry fizyczne platformy**	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Maksymalny pobór mocy: 60 W. • Minimalny zakres temperatury pracy: 0-40^{o}C.
	Interfejsy sieciowe - wymagania minimalne	1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 48 porty GE RJ-45. e) 4 porty 10 GE SFP+.
	Zarządzanie	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
	Parametry wydajnościowe	• Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów.

		• Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
	Wymagane funkcje	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci.

		2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. /12 m-cy.
	Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

4. Minimalne wymagania techniczne dla przedmiotu zamówienia – System operacyjny

Asortyment	**Parametr**	**Wartość minimalna**
1.	2.	3.
System Operacyjny operacyjny	w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	
		Zainstalowany system operacyjny Windows 10 lub 11 Professional, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego(**dotyczy dostawy systemu z komputerem**), w polskiej wersji językowej lub równoważny spełniający następujące wymagania minimalne poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Umożliwia integrację z domeną Active Directory pozwalającą na wdrożenie jednolitej polityki bezpieczeństwa dla wszystkich komputerów w sieci. 2. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 3. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 4. 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, 5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 6. Wbudowany system pomocy w języku polskim. 7. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego 8. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 9. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 10. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania

		problemu z komputerem. 11. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 12. automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 13. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 14. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 15. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 16. Wbudowany mechanizm wirtualizacji typu hypervisor. 17. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 18. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 19. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 20. 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.). 21. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 22. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 23. Możliwość tworzenia wirtualnych kart inteligentnych. 24. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu(SecureBoot) 25. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 26. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 27. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 28. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń Licencja na system operacyjny musi być nieograniczona w czasie. Klucz licencyjny zapisany trwale w BIOS, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.

5. Minimalne wymagania techniczne dla przedmiotu zamówienia – System Kopi Bezpieczeństwa

Asortyment	Parametr	Wartość minimalna
1.	2.	3.
NAS	Procesor	Czterordzeniowy procesor 1,7 GHz
	Architektura procesora	64-bitowy ARM
	Koprocesor arytmetyczny FPU	Tak
	Pamięć systemowa	4 GB UDIMM DDR4 (1 x 4 GB)
	Maksymalna pojemność pamięci	16 GB (1 x 16 GB)
	Gniazdo pamięci	1 x Long-DIMM DDR4
	Pamięć flash	512 MB (ochrona systemu operacyjnego przed podwójnym rozruchem)
	Wnęka dysków	8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
	Kompatybilność dysków	3,5-calowe wnęki: 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA
	Dysk wymieniany podczas pracy	Tak

	Gniazdo dysku M.2 SSD	Opcjonalne poprzez kartę PCIe
	Obsługa przyspieszenia pamięci podręcznej SSD	Tak
	Port 2,5 Gigabit Ethernet (2,5G/1G/100M)	2 (także obsługa 10M)
	Port 10 Gigabit sieci Ethernet	2 x 10GbE SFP+
	Wake on LAN (WOL)	Tak - Tylko port 2,5GbE
	Ramka Jumbo	Tak
	Gniazdo PCIe	1 Gniazdo 1: PCIe Gen 2 x2Ograniczenia przepustowości PCIe spowodują pogorszenie wydajności NAS 10GbE.
	Port USB 3.2 Gen 1	4
	Kształt	2U, do montażu stelażowego
	Wskaźniki LED	HDD 1–8, stan, LAN, Rozszerzanie pamięci masowej
	Przyciski	Zasilanie, reset
	Wymiary (wys. x szer. x gł.)	89 × 482 × 534 mm
	Maks. Liczba jednoczesnych połączeń (CIFS) - z max. Pamięć	700

	W zestawie przesuwne szyny montażowe	Tak

6. Minimalne wymagania techniczne dla przedmiotu zamówienia – UPS

Asortyment	**Parametr**	**Wartość minimalna**
1.	2.	3.
UPS	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
	Moc znamionowa	3 kVA / 2,7 kW
	Wyjściowy współczynnik mocy (PF)	0,9
	Napięcie wejściowe	230 Vac
	Sposób zasilania	Plug&Play Gniazdo w standardzie IEC 320
	Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie	160 – 276 Vac
	Tolerancja napięcia wejściowego przy	120 – 276 Vac

	obciążeniu mniejszym od 70%; bez przechodzenia na baterie	
	Częstotliwość wejściowa	Wymagana 40-70 Hz
	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 92%
	Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
	Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
	Napięcie wyjściowe	230 Vac
	Częstotliwość wyjściowa	50/60Hz (programowalna)
	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)	Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny
	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane

	Czas podtrzymania	Min. 18 minuty dla 2700 W
	Wymiary zestawu w szafie rack, Wymagane szyny do montażu	2 U, Tak
	Waga	Do 70 kg
	Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10 lat,
	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%
	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
	Stabilność częstotliwości wyjściowej:	bez synchronizacji: ± 0,05%
	Współczynnik szczytu	3:1
	Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną	Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości
	Złącze interfejsów	RS232, USB, REPO
	Gniazda wyjściowe IEC320 na zasilaczu UPS	Wymagane minimum gniazd 8 szt x IEC 320-C13

	Karta sieciowa SNMP	Wymagane
	Interfejs EPO (do wyłącznika ppoż.)	Wymagane
	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
	Poziom hałasu w odległości 1m,	< 46 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
	Możliwość regulacji z oprogramowania tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
	Zabezpieczenie przed zwrotnym podaniem napięcia niebezpiecznego do obwodu zasilającego UPS	Wymagane
	Normy środowiskowe	Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
	Instrukcja w języku polskim	Wymagane

	Wsparcie techniczne	1 Oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji. Jeżeli oferowana jest niestandardowa, rozszerzona gwarancja to wymagane jest by realizowana była wyłącznie przez serwis producenta - należy przedstawić odpowiednie oświadczenie producenta oferowanego sprzętu. 2. Oświadczenie producenta urządzenia, iż w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem

7.Minimalne wymagania techniczne dla przedmiotu zamówienia – Oprogramowanie biurowe

Asortyment	**Parametr**	**Wartość minimalna**
1.	2.	3.
Oprogramowanie biurowe	Pakiet biurowy (wraz z licencją na czas nieokreślony, kluczem instalacyjnym tego oprogramowania): Office 2019 PL lub innego oprogramowania biurowego równoważnego, zawierającego co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej oraz kalendarza, które charakteryzuje się następującymi cechami: całkowicie zlokalizowany w języku polskim interfejs, system komunikatów i podręcznej kontekstowej pomocy technicznej (w tym także on-line) w	

	pakiecie, możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego), możliwość zdalnej instalacji komponentów, możliwość prowadzenia dyskusji oraz subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach, oraz publikowanie dokumentów wprost z komponentów pakietu np. arkusza kalkulacyjnego, w systemach pocztowych - możliwość delegacji uprawnień do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji, możliwość blokowania niebezpiecznej lub niechcianej poczty, automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi, potwierdzanie dostarczenia do skrzynki adresata oraz potwierdzanie otwarcia poczty u adresata, współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników, wsparcie dla formatu XML w podstawowych aplikacjach, możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów, automatyczne wyróżnianie i aktywowanie hyperlinków w dokumentach podczas edycji i odczytu,	

	możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych, możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem CryptoAPI, możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu, prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach:.doc, .docx, xls,.xlsx, ppt, .pptx, .pps, .ppsx, w tym obsługa formatowania, wykonywanie i edycję makr oraz kodu zapisanego w języku Visual Basic for Application w plikach xls, xlsx, formuł, formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010 bez utraty danych oraz bez konieczności reformatowania dokumentów, prawidłowe otwieranie i zapisywanie plików o formatach doc, docx, xls, xlsx, .ppt, pptx. .pps, .ppsx bez utraty parametrów i cech użytkowych zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb,	

	obrazków, wykresów, odstępy między tymi obiektami i kolorów, działające makra, prawidłowa współpraca zapis, odczyt z plikami danych programów pocztowych w formacie .pst oraz prawidłowy import z formatu .dbx, wszystkie komponenty oferowanego pakietu biurowego (edytor, arkusz, klient poczty, kalendarz oraz program do prezentacji) muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi, poprawna praca w systemach operacyjnych w które może być wyposażony zamawiany zestaw, tj. 64-bitowych z rodziny Windows 7, Windows 8, Windows 8.1, Windows 11 lub równoważny, w przypadku zaoferowanego oprogramowania równoważnego należy podać dokładną nazwę i wersję oferowanego produktu, zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.	

8. Minimalne wymagania techniczne dla przedmiotu zamówienia – Serwer

Asortyment	Parametr	Wartość minimalna
1.	2.	3.
Serwer		
	Obudowa	Wysokość maksymalnie 2U RACK 19 cali wraz z szynami montażowymi oraz-zestawem ułatwiającym wyprowadzenie przewodów z tyłu serwera Opcjonalny czujnik otwarcia obudowy. Zainstalowany moduł TPM 2.0 Zdejmowany panel przedni wyposażenia w zamek i chroniącym przed nieuprawionym dostępem do dysków.
	Procesor	Jeden procesor 16 rdzeniowy, x86 - 64 bity, osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 235 punktów. Wynik testu dla konfiguracji 2 procesorowej oferowanego serwera musi być opublikowany na stronie http://spec.org w dniu złożenia oferty. Płyta główna wspierająca zastosowanie procesorów do 40 rdzeni, mocy do min. 270W
	Pamięć operacyjna	64 GB RDIMM DDR4 3200 MT/s w modułach o pojemności 32 GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej). Obsługa zabezpieczeń: Advanced ECC/SDDC Rank sparing (online spare), Demand scrubbing Patrol scrubbing, Failed DIMM isolation Memory thermal control, DIMM address/control bus parity protection Mirrored memory with advanced ECC support.
	Sloty rozszerzeń	Serwer musi posiadać w standardzie minimum 3 sloty PCI-Express Gen4, w tym jeden slot działający z prędkością x16 (bus width) pełnej wysokości. Możliwość rozbudowy do sumarycznej ilości slotów PCI-E: • Minimum 2 sloty PCI-Express Gen4 działające z prędkością x16 (bus width), w tym jeden slot pełnej

		wysokości. • Minimum 2 sloty PCI-Express Gen4 dwa działające z prędkością x8 (bus width). Powyższa konfiguracja musi być dostępna przy konfiguracji dwu procesorowej serwera. Serwer musi posiadać dedykowany slot rozszerzeń interfejsów sieciowych, niezajmujący dostępnych slotów PCI-Express oraz dedykowany slot dla kontrolera RAID niezajmujący dostępnych slotów PCI-Express.
	Dysk twardy	Możliwość zainstalowania do 12 dysków typu Hot Swap, SAS/SATA/SSD, 3.5” z możliwością rozbudowy o kolejne cztery dyski 3.5” Zainstalowane dyski: 2 szt. dysków 3.5” SATA SSD MU o pojemności nie mniejszej niż 960GB każdy 4 szt. dysków 3.5” SATA HDD 7.2k o pojemności nie mniejszej niż 6TB każdy Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Możliwość wyposażenia serwera w kartę RAID wyposażoną w dwa dyski M.2 NVMe o pojemności 480GB każdy skonfigurowane w RAID 1. Dyski nie mogą zajmować slotów opisanych powyżej.
	Kontroler	Serwer wyposażony w kontroler sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. Obsługujący dyski SAS/SATA/SSD. Kontroler umożliwiający pracę z dyskami w trybach RAID i HBA jednocześnie.
	Interfejsy sieciowe	Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Dedykowany port 1Gb RJ45 dla karty zarządzającej.
	Karta graficzna	Zintegrowana karta graficzna.
	Porty	Złącza USB: min. 4 porty USB 3.0 w tym 2 szt. wewnątrz obudowy oraz 2 porty USB 3.0 z tyłu serwera VGA z tyłu serwera Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy o: - dodatkowy port typu DisplayPort lu HDMI dostępny z przodu serwera - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45

	Zasilacz	2 szt. typu Hot-plug, redundantne, każdy o mocy minimum 800W.
	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug Model serwera zgodny standardem ASHRAE Class A4 z możliwością pracy w temperaturze otoczenia równej 45st.C.
	Napęd	Możliwość instalacji zewnętrznego napędu DVD-RW
	Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez o dedykowany port RJ45 z tyłu serwera lub o dostęp do karty możliwy: o z poziomu przeglądarki webowej (GUI) o z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) o z poziomu skryptu (XML/Perl) o poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji

		• konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: o tworzenie i konfiguracja grup serwerów o sterowanie zasilaniem (wł/wył) o ograniczenie poboru mocy dla grupy (power caping) o aktualizacja oprogramowania (firmware) o wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
	System monitorowania i analizowania konfiguracji serwerów	Dostęp do systemu wymagany jest dla każdego oferowanego serwera. Jeżeli wymaga to dodatkowych licencji, to należy takie licencje dostarczyć. System musi być w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT Zamawiającego. Platforma wspierana uczeniem maszynowym i analizą predykcyjną, zapewniająca automatyczne zbieranie i analizę danych z modułów zarządzania serwerami w celu monitorowania, analizy ich pracy i porównania zachowania serwerów z danymi z referencyjnej bazy danych wszystkich podłączonych do tego systemu serwerów. System musi zapewniać: - scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); - informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; - prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; - rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom; - analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania; - prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach. - zalecenia dotyczące eliminacji źródeł/przyczyn problemów wydajnościowych serwerów.
	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server min. 2016, 2019, 2022 Red Hat Enterprise Linux (RHEL) min. 7.9, 8.2, 9 SUSE Linux Enterprise Server (SLES) min. 12, 15

		VMware ESXi min. 6.7, 7.0 Oracle Linux 8 Ubuntu 20.04 LTS, 22.04 LTS Oferowany serwer musi znajdować się na liście VMware HCL dla ESXi 7.0 oraz na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2016, 2019, 2022.
	System Operacyjny	System operacyjny w najnowszej wersji pozwalający na uruchomienie min. dwóch zalicencjonowanych wirtualnych maszyn z odpowiednią ilością zalicencjonowanych rdzeni procesora. Spełniający poniższe wymagania: a) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. b) 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. c) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. d) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. e) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. f) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. g) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. h) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. i) Możliwość uruchamianie aplikacji internetowych wykorzystujących techologię ASP.NET. j) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. k) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. l) Graficzny interfejs użytkownika. m) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. n) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). o) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

		p) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. q) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). r) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: i) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. ii) 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. iii) Zdalna dystrybucja oprogramowania na stacje robocze. iv) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. v) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: (1) dystrybucję certyfikatów poprzez http, (2) konsolidację CA dla wielu lasów domeny, (3) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. vi) Szyfrowanie plików i folderów. vii) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). viii) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. ix) Serwis udostępniania stron WWW. x) Wsparcie dla protokołu IP w wersji 6 (IPv6). xi) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, s) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. t) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). u) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. v) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. w) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; x) Materiały edukacyjne w języku polskim. Wraz z serwerem wymagane jest dostarczenie trzydziestu pięciu licencji (CAL) na użytkowana.

	Wsparcie techniczne	Oferowany sprzęt powinien posiadać minimalne wsparcie serwisowe na okres co najmniej trzech lat realizowanym w miejscu instalacji sprzętu. Serwis świadczony przez producenta serwera w trybie 8x5. Czas reakcji serwisu w następnym dniu roboczym od momentu zgłoszenia usterki w miejscu instalacji serwera. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.-załączyć oświadczenie producenta Deklaracja zgodności CE.

9. Minimalne wymagania techniczne dla przedmiotu zamówienia – UTM

Asortyment	**Parametr**	**Wartość minimalna**
1.	2.	3.
UTM	**Wymagania Ogólne**	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

		W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
	Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
	Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 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 Gbps. 6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.

		7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
	Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być 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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
	Polityki, Firewall	1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

		8. Amazon Web Services (AWS). 9. Microsoft Azure 10. Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
	Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • 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. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać 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 musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN
	Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
	Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

		2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
	Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
	Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
	Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie,

		zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
	Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

		3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
	Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
	Gwarancja oraz wsparcie	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać

		również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

10. Minimalne wymagania techniczne dla przedmiotu zamówienia – Dysk HDD

Asortyment	**Parametr**	**Wartość minimalna**
1.	2.	3.
Dysk	HDD	4 SZT.
	Pojemność dysku	4 TB.
	Interfejs	SATA III (6 Gb/s)
	Pamięć podręczna	256 MB
	Prędkość obrotowa	5400 obr./min

	Format	3.5”
	Nominalny czas pracy	1000 000 000 godzin
	Dodatkowe wymagania	Dyski muszą znajdować się na oficjalnej liście kompatybilności producenta macierzy/serwera NAS