SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

W projekcie „CYFROWA GMINA" współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego, Program Operacyjny Polska Cyfrowa (POPC) na lata 2014-2020, pakiet REACT-UE

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

Informacje ogólne

1. W przypadkach, kiedy w 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 przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne".

3. Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ.
Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

4. Dla jednoznacznej identyfikacji oferowanego sprzętu należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego sprzętu. Zamawiający wymaga również podania faktycznych parametrów sprzętu, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany sprzęt spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane urządzenia spełniają wymagania Zamawiającego.

5. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

6. Dostarczany sprzęt musi być fabrycznie nowy i pochodzić z najnowszych linii produktowych.

7. Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające itp).

8. Sprzęt musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności bezterminowymi licencjami na używanie tych funkcjonalności.

9. Ofertowany sprzęt musi posiadać Certyfikaty ISO1043, ISO9001, ISO14001, deklaracja producenta sprzętu zgodności z CE lub dokument równoważny.
Oferowany sprzęt musi spełniać wymogi dyrektywy WEEE 2002/96/EC z dnia 27 stycznia 2003 r. dotyczącej odpadów elektrycznych i elektronicznych.

Oferowany sprzęt musi spełniać wymagania dyrektywy 2002/95/EC z dnia 27 stycznia 2003 na temat zakazu użycia niebezpiecznych substancji w wyposażeniu elektrycznym i elektronicznym.

SPRZĘT I OPROGRAMOWANIE

Lp.	Nazwa	Ilość
1.	Komputer stacjonarny typu All-In-One wraz z systemem operacyjnym	17 szt.
2.	Serwer plików NAS QNAP lub równoważny	1 szt.
3.	Serwer wraz z systemem operacyjnym i licencjami dostępowymi	1 kpl.
4.	Zasilacz awaryjny UPS	1 szt.
5.	Zasilacz awaryjny UPS	15 szt.
6.	Pieczęć elektroniczna	1 szt.
7.	Dodatkowe moduły do oprogramowania antywirusowego ESET	1 kpl.
8.	Oprogramowanie biurowe	17 szt.
9.	Rozbudowa zabezpieczeń logicznych Firewall – zakup Urządzenia UTM	1 szt.
10.	Laptop wraz z systemem operacyjnym	7 szt.

1. Komputer stacjonarny typu All-In-One wraz z systemem operacyjnym (17 szt.)

Nazwa komponentu	Minimalne wymagane parametry techniczne komputerów
Typ	Komputer stacjonarny typu All In One
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, programów dziedzinowych, dostępu do Internetu oraz poczty elektronicznej.
Procesor	(np. Intel Core i3, Intel Core i5, AMD Ryzen 3, AMD Ryzen 5) lub równoważny osiągający minimum: Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min.- 5000 punktów CPU Mark http://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	8GB DDR4
Pamięć masowa	Dysk SSD min. 256GB
Obudowa	Zintegrowana z monitorem (AIO) musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)
Ekran	Przekątna: min. 23” Rozdzielczość: min. FHD (1920x1080) Częstotliwość odświeżania ekranu: MIN: 60 Hz Matryca: podświetlenie LED, format 16:9, antyodblaskowa

Wydajność grafiki	Zintegrowana z procesorem, pamięć współdzielona z pamięcią RAM
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane głośniki, wbudowana kamera
Zgodność z systemami operacyjnymi i standardami	Oferowany model komputera musi poprawnie współpracować z zamawianymi systemami operacyjnymi .
System operacyjny	1. System operacyjny dla komputerów AiO, 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; MS Visio 2007, 2010, 2016; 3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 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: - 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
Interfejsy	**Wbudowane porty:** - wejście oraz wyjście liniowe oraz wejście mikrofonowe - 1xRJ-45, - 6 portów USB wyprowadzonych na zewnątrz obudowy, Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. - 2 porty HDMI - Karta sieciowa 10/100/1000 zintegrowana z płytą główną - karta WiFi 802.11 a/b/g/n/ac - Bluetooth w wersji 5.0 - gniazdo kart pamięci SD - klawiatura USB w układzie polski programisty - mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
Warunki gwarancji	Gwarancja producenta **minimum 24 miesiące**,

2. Serwer plików NAS QNAP lub równoważny (1 szt.)

Specyfikacja sprzętowa	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Zainstalowane dyski	2 x 2TB (dedykowane dla urządzeń NAS)
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
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.
Zasilanie	Max. 250 W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
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 LXC 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	3 lata

3. Serwer wraz z systemem operacyjnym i licencjami dostępowymi (1 kpl.)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
	Obudowa	rozmiar: 1U Ilość obsługiwanych dysków i kieszeni: 4 sztuk 3,5” (Hot-Plug, HOTSWAP)
	Procesor:	1 sztuka (zainstalowane na płycie głównej wraz z dedykowanym systemem chłodzenia): • Częstotliwość: MIN: 3,4 GHZ • Liczba rdzeni: MIN: 8 • Liczba wątków: MIN: 16 • Znamionowa moc termiczna (TDP) MAX: 80W Dedykowany system wentylacji i chłodzenia
	Płyta główna	Dedykowana dla procesora, w rozmiarze microATX 9.6 x 9.6”, obsługująca pamięć RAM do 128 GB o taktowaniu przynajmniej 2666 MHz DDR4, **Posiadająca:** - 6 szt. porty SATA3 - obsługująca RAID 0,1,5,10 - 6 szt. USB 2.0 - 5 szt. USB 3.1 - slot PCI-E 3.0 x8 - 2 gniazda PCI-E x4 - gniazdo M.2

		BIOS – UEFI 256Mb - 2xVGA z czego jeden na panelu przednim
	Pamięć:	Wielkość: 64 GB (2 x 32GB) Rodzaj: DDR4, taktowanie MIN: 3200 MHz
	Dyski, kontrolery, interfejsy	- kontroler SAS3 z procesorem o taktowaniu minimum 1.2 GHz, obsługujący RAID 0, 1 i 10, low profile, 12Gb/s per port, wspierający przynajmniej 63 urządzenia pamięci masowej, typ portu rozszerzeń PCI Express 3.0 - możliwość zamontowania dodatkowej karty rozszerzeń PCI-E 3.0 x8 (riser card) Zainstalowane dyski twarde (4 sztuk): • 3 x 3,5” HDD SAS 12 Gb/s, 7200 obr. o pojemności MIN: 4TB (Hot-Plug) każdy zamontowany w kieszeni o wymiarach 3,5”, przeznaczenie: do pracy w serwerach, emulacja 512 (512e) • 1 x 2,5” SSD SATA3 6 GB/s o pojemności MIN: 480 (Hot-Plug) zamontowany w kieszeni o wymiarach 3,5”, szybkość przesyłu danych: MIN: 520 MB/s, MTBT: 2000000 h
	Sieć	Zainstalowane karty sieciowe (kompatybilne): • MIN: 1 karta MIN: Dual-Port 1 GbE On-Board LOM • MIN: 1 karta MIN: Dual Port 10 GbE BaseT (SFP+) umożliwiająca transfer danych na poziomie nie mniejszym niż 10 Gbps
	Zasilacz	Zasilacz (zainstalowane): 2 sztuki: Hot-plug, redundantne (1+1), MIN: 500W
	System Operacyjny	Np. Windows Server 2022 Standard lub równoważny Opis wymagań technicznych, funkcjonalnych, jakościowych - równoważnych: Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,

		d) 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, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. Certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) 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), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline - bez dostępnego

		połączenia sieciowego z domeną 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. 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 mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) 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, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

	Licencje dostępowe	Zamawiający wymaga dostawy licencji umożliwiającej dostęp do zakupionego w ramach niniejszego postępowania serwera, spełniająca wymagania minimalne: 1. System powinien umożliwiać uwierzytelnienie i dostęp do usług serwerowych użytkownikom, pracownikom w sieci lokalnej jak i poza nią. 2. Typ licencji: **USER CAL** 3. Okres licencji: **wieczysta** 4. Liczba użytkowników: **25 szt.**
	Zarządzanie	· Zarządzanie zdalne przez wydzielony interfejs 1 GbE · Wbudowany system zdalnego zarządzania IPMI 2.0 lub oprogramowanie zapewniające podobną funkcjonalność niezależne od zainstalowanego systemy operacyjnego. o zdalne monitorowanie i informowanie o statusie serwera – minimum o prędkości obrotowej wentylatorów, poborze prądu przez serwer, wartości napięcia i temperatury, o zdalne włączanie i wyłączanie serwera (power on/power off), o zdalny dostęp do graficznego interfejsu Web modułu zarządzającego i interfejsu CLI ze wsparciem dla szyfrowania połączeń SSLv3 i ssh wraz z autentykacją i autoryzacją użytkownika, o dostęp do wirtualnej konsoli graficznej z obsługą myszy i klawiatury, bez konieczności instalowania dodatkowych modułów do przeglądarki (np. realizowany za pomocą HTML5) o mapowanie zdalnych wirtualnych napędów, o wsparcie dla SNMP, IPMI2.0, VLAN tagging, · wsparcie dla powiadomień e-mail w przypadku awarii lub zmiany konfiguracji sprzętowej oraz przekroczenia zadanych progów parametrów pracy
	Certyfikaty	Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC

4. Zasilacz awaryjny UPS (1 szt.)

Moc wyjściowa (pozorna / czynna)	minimum 3000 VA
	minimum 3000 W
Topologia	VI (line interactive)
Typ obudowy	Rack / Tower
Chłodzenie	Wymuszone, wewnętrzne wentylatory
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	178 ÷ 281 V AC ± 2 %

Częstotliwość znamionowa napięcia wejściowego	50 Hz
Zakres częstotliwości i tolerancja	45 ÷ 55 Hz ± 1 Hz
Progi przełączania: sieć – UPS	178 ÷ 281 V AC ± 2 %
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	195 ÷ 253 V AC ± 2 %
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa	230 V AC ± 5 %
Automatyczna regulacja napięcia (AVR)	± 10 %
Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej)	Sinusoidalny / Tak jak na wejściu
Częstotliwość znamionowa napięcia wyjściowego	50 Hz
Filtracja napięcia wyjściowego	Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy
Progi przełączania: UPS – sieć	183 ÷ 276 V AC ± 2 %
Czas przełączenia na pracę rezerwową	< 3 ms
Czas powrotu na pracę sieciową	0 ms
Przeciążalność	> 105% - 15 s (wyłączenie UPS)
Akumulatory wewnętrzne	minimum 12 V / 7 Ah VRLA
możliwość podłączenia zewnętrznego modułu bateryjnego	wymagana
Czas podtrzymania wyłącznie z baterii wewnętrznych dla obciążenia 3000W	minimum 3 min
Wymiary – Tower (wys. X szer. X gł.)	nie większe niż 440 x 132 x 630 mm
Masa zasilacza	nie większa niż 43 kg
Zabezpieczenie wejściowe	Przeciwzwarciowe – Bezpiecznik automatyczny
	16 A / 250 V AC
	Przeciwprzepięciowe
Zabezpieczenie wyjściowe	Elektroniczne – przeciwzwarciowe i przeciążeniowe
Zabezpieczenia wejścia DC (akumulatory wewnętrzne)	Zabezpieczenie nadprądowe
Zabezpieczenia DC (zewnętrzny moduł bateryjny)	Zabezpieczenie nadprądowe
Przyłącza wyjściowe (liczba i typ gniazd)	minimum 9 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym)
Sygnalizacja	Akustyczno – optyczna; graficzny wyświetlacz LCD, dioda LED
Interfejsy komunikacyjne	USB HID, SNMP/HTTP
Gniazdo na dodatkowe karty rozszerzeń	wymagane
Oprogramowanie monitorująco-zarządzające	oprogramamowanie w języku polskim do zarządzania i monitorowania pracy UPS .
	możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP)

	możliwość edycji nazw urządzeń na liście monitorowanych UPSów
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego	wymagane
Możliwość aktualizacji oprogramowania firmware przez użytkownika	wymagane
Deklaracje	CE
Normy	PN-EN 62040-1:2009, PN-EN 62040-2:2008
Gwarancja	min 36 miesięcy na elektronikę i 24 miesiące na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
	naprawa urządzenia do 3 dni roboczych
	serwis realizowany w systemie door to door
	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań
	oświadczenie producenta o spełnieniu minimlanych wymaganych parametrów specyfikacji
	karta katalogowa oferowanego sprzętu

5. Zasilacz awaryjny UPS (15 szt.)

Parametr	Wymagania minimalne
moc pozorna	min. 550VA
moc rzeczywista	min. 330W
Technologia	VI (line interactive)
Typ obudowy	wolnostojąca
praca sieciowa	

Napięcie wejściowe	162 ÷ 290 V AC ± 7 V
Częstotliwość napięcia wejściowego	40 ÷ 70 Hz ± 1 Hz
Zakres napięcia wyjściowego	230 V AC ± 10 %
Kształt napięcia wyjściowego	Schodkowa aproksymacja sinusoidy / Tak jak na wejściu
Progi przełączania sieć – UPS	162 ÷ 290 V AC ± 7 V
Czas przełączania sieć – UPS	<6ms
praca bateryjna	
Napięcie wyjściowe	~230V ± 10%
Częstotliwość napięcia wyjściowego	50 / 60 Hz ± 1%
Kształt napięcia wyjściowego na pracy bateryjnej	Schodkowa aproksymacja sinusoidy
Progi przełączania UPS – sieć	~172 ÷ 280 V ± 7 V
Przeciążalność	> 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna)
Zabezpieczenie wyjściowe przeciwzwarciowe	elektroniczne
Zabezpieczenie wyjściowe przeciążeniowe	elektroniczne
Czas podtrzymania dla obciążenia 165W	minimum 6 min
akumulatory wewnętrzne	minimum 12V5Ah; szczelne, bezobsługowe VRLA
pozostałe	
Ilość i typ gniazd wyjściowych	minimum 2 gniazda z podtrzymaniem standardu PL (z bolcem uziemiającym) + minimum 1 gniazdo z podtrzymaniem standardu IEC 320 C13 (10 A)
Sygnalizacja	Akustyczno-optyczna
	Dioda sygnalizująca minimum pracę sieciową, bateryjną, niski poziom baterii, przeciążenie, awarię
	Sygnalizacja akustyczna informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu, awarii
Zimny Start	tak
Interfejs komunikacyjny	USB HID (kabel w komplecie)
Automatyczna regulacja napięcia AVR	wymagana
Waga UPS	do 4kg
wymiary	nie większe niż: wysokość 160mm; szerokość 85mm; głębokość 255mm
gwarancja	min 24 miesiące na elektronikę i 12 miesięcy na akumulatory;
serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
	serwis realizowany w systemie door-to-door
oprogramowanie	oprogramamowanie w języku polskim do zarządzania i monitorowania pracy UPS .
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
	możliwość edycji nazw urządzeń na liście monitorowanych UPSów

	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań
	deklaracja CE producenta sprzętu
oświadczenia / dokumenty	oświadczenie producenta o spełnieniu minimlanych wymaganych parametrów specyfikacji
	karta katalogowa oferowanego sprzętu

6. Pieczęć elektroniczna (1 szt.)

Nazwa komponentu	Wymagane minimalne parametry techniczne
Opis	- Pieczęć elektroniczna musi umożliwić tworzenie oficjalnych dokumentów firmowych i urzędowych w formie elektronicznej, zachowując równocześnie w świetle przepisów prawa ich pełną moc prawną i wartość dowodową. - Oprócz wszystkich innych wymaganych cech kwalifikowalnej pieczęci elektronicznej, powinna zawierać kwalifikowalny znacznik czasu, wykorzystywany w ilości min 5000 szt. na miesiąc, oprogramowanie i sterowniki dla systemu WINDOWS 10 /11, kartę z pieczęcią wbudowaną w czytnik kart z możliwością podłączenia do portu USB. - Certyfikat wspierany przez Adobe
Zastosowanie	Urzędy administracji publicznej: • Zarządzenia • Uchwały • Dokumenty księgowe • Regulaminy • Zamówienia / Protokoły odbioru • Akty prawne • Postanowienia • Faktury • Korespondencja wychodząca • Decyzje i inne dokumenty urzędowe
Okres ważności	Min. 2 lata

7. Dodatkowe moduły do oprogramowania antywirusowego ESET (1 kpl.)

Zamawiający korzysta z oprogramowania ESET . W związku chęcią podniesienia bezpieczeństwa na urządzeniach końcowych, zamawiający chce zakupić modyfikację licencji ESET Endpoint Security do ESET PROTECT Essential ON-PREM dla 40 użytkowników na okres 12 miesięcy.
1. Zaoferowane licencje oprogramowania muszą być oryginalne i pochodzić z legalnego, autoryzowanego kanału sprzedaży na Rynek Unii Europejskiej.
2. Zaoferowane oprogramowanie musi być objęte gwarancją w całym okresie obowiązywania licencji.

8. Oprogramowanie biurowe (17 szt.)

Oprogramowanie biurowe	Pakiet oprogramowania biurowego typu np. MS Office Home and Business 2021 PL lub równoważny:

	Opis wymagań technicznych, funkcjonalnych, jakościowych - równoważnych: 1. W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania. 2. Oferując rozwiązanie równoważne dla oprogramowania wymienionego przez Zamawiającego, Wykonawca zobowiązany jest wykazać, że rozwiązania równoważne zachowują cechy techniczne, funkcjonalne i jakościowe w stosunku do oprogramowania wskazanego przez Zamawiającego. 3. Zamawiający wymaga udzielenia licencji na oprogramowanie wchodzące w zakres przedmiotu zamówienia oraz dopuszcza oferowanie oprogramowania o szerszym zakresie funkcjonalnym od wymaganego. 4. Przez wykazanie równoważności Zamawiający rozumie wykonanie stosownych porównań i analiz. Wyniki porównań i analiz należy załączyć do oferty. 5. Wykonawca odpowiada za wszelkie wady prawne dostarczonego oprogramowania i licencji, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem oprogramowania do obrotu na terytorium Rzeczypospolitej Polskiej; ewentualne roszczenia osób trzecich wynikające z praw autorskich lub patentowych, dotyczące przedmiotu dostawy, będą dochodzone bezpośrednio od Wykonawcy. 6. Produkty muszą być w pełni kompatybilne z posiadanym przez Zamawiającego oprogramowaniem (MS Office) bez potrzeby dodatkowej edycji, formatowania, konwertowania i modyfikowania. **7. Nie dopuszcza się zastosowania licencji zbiorczej.** **8. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych lub dodatkowych opłat w okresie używania zakupionego produktu.** 9. Zamawiający dopuszcza dostawy licencji na oryginalnych kartach z kluczem produktu lub licencji w wersji cyfrowej. 10. Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta. 11. Wymagane licencje muszą pozwalać na przenoszenie pomiędzy stacjami roboczymi. 12. Oprogramowanie musi posiadać możliwość automatycznego odzyskiwania dokumentów elektronicznych w wypadku nieoczekiwanego zamknięcia aplikacji, np. w wyniku wyłączenia zasilania komputera.

	13. Oprogramowanie musi zapewniać prawidłowe odczytywanie i zapisywanie danych, w tym obsługę formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office , bez utraty danych oraz bez konieczności reformatowania dokumentów. 14. Oprogramowanie musi zawierać narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 15. Wszystkie aplikacje w pakiecie oprogramowania biurowego muszą być integralną częścią tego samego pakietu, muszą współpracować ze sobą. 16. Wykonawca może udostępnić w wersji elektronicznej pliki instalacyjnego zaproponowanego produktu. 17. Wykonawca musi udostępnić pliki i wersje produktu w ich najnowszych wydaniach i/lub załączyć wszelkie pliki aktualizacyjne czy tzw. servicepack(i). 18. Nie dopuszcza się licencji wykorzystywanych wcześniej na innych stacjach roboczych. Licencje nie mogą być nigdy wcześniej aktywowane.

9. Rozbudowa zabezpieczeń logicznych Firewall – zakup Urządzenia UTM (1 szt.)

	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:
   - 5 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 700 tys. jednoczesnych połączeń oraz 32 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 protokołem AES z kluczem 128 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. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

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:

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 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 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.

2. Rozszerzone wsparcie serwisowe AHB/SOS

System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania powinny być potwierdzone dokumentami:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

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.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

10. Laptop wraz z systemem operacyjnym (7 szt.)

Atrybut	Wymagania
Laptop	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.

	Dostarczany sprzęt musi być fabrycznie nowy.
Ekran	15.6 FHD IPS (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nits. Kąt otwarcia matrycy min.180 stopni
Obudowa	Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.180 stopni. W obudowie wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego.
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs PCIe oraz SATA III (6 Gb/s) do obsługi dysków twardych.
Wydajność komputera	Oferowany komputer przenośny musi osiągać w teście wydajności : SysMark25– wynik min. 600 pkt – test z przeprowadzonej konfiguracji na wezwanie Zamawiającego załączyć do oferty. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć operacyjna	Min 8GB z możliwością rozbudowy do 16GB, rodzaj pamięci min. DDR4.
Dysk twardy	Min. 256GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 2 GB pamięci. Karta graficzna osiągająca w teście SysMark25 Creativity wynik min. 550 pkt. – test z przeprowadzonej konfiguracji na wezwanie Zamawiającego załączyć do oferty.
Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 2W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), wbudowana kamera 720p.
Karta sieciowa	Zintegrowana z płytą główną 10/100/1000 – RJ45
Porty/złącza	3xUSB w tym minimum 2xUSB 3.2, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI, RJ-45. Złącze bezpieczeństwa typu Kensington lub Noble.
Klawiatura	Klawiatura wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym.
WiFi	Wbudowana karta sieciowa, pracująca w standardzie AC

Bluetooth	Wbudowany moduł Bluetooth 4.2
Bateria	Bateria pojemności min. 35Whr. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii mi. 8 godzin, potwierdzony przeprowadzonym testem MobileMark 25 Battery Life [do oferty załączyć wydruk przeprowadzonego testu lub link publikacji na stronie BAPCO, w oferowanej konfiguracji, na wniosek zamawiającego]
Zasilacz	Zasilacz zewnętrzny max 65W z kablami połączeniowymi.
BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS - nr seryjnym komputera - ilości pamięci RAM - typie procesora i jego prędkości -modele zainstalowanych dysków twardych Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: Możliwość ustawienia hasła dla twardego dysku Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password Możliwość ustawienia hasła Administratora i użytkownika BIOS Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej, Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
Bezpieczeństwo	- złącze Kensington Lock, - Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego (TPM 2.0). Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer

	kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
Certyfikaty i standardy	Certyfikat ISO9001 oraz 50 001 dla producenta sprzętu (należy załączyć do oferty) ENERGY STAR - certyfikat lub wydruk ze strony http://www.eu-energystar.org lub http://www.energystar.gov 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
Waga/Wymiary	Waga urządzenia z baterią podstawową maksymalnie 2,0 kg
System operacyjny – w formularzu oferty trzeba podać nazwę oferowanego oprogramowania	Np. Windows 10 Home 64 bit lub równoważny System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: Dostępne dwa rodzaje graficznego interfejsu użytkownika: Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 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, Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim Wbudowany system pomocy w języku polskim. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. Klucz produktu przypisany do komputera aby przy ponownej reinstalacji systemu nie było konieczności wpisywania klucza.
Gwarancja	2-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego.