Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 1 do SWZ

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup i dostawa fabrycznie nowego, nieużywanego, nieuszkodzonego, nieobciążonego prawami osób lub podmiotów trzecich sprzętu komputerowego, zbiorczego UPS oraz oprogramowania, spełniającego poniższe minimalne parametry techniczne:

I część komputery stacjonarne, monitory, komputery przenośne, oprogramowanie		
Lp.	**SPECYFIKACJA TECHNICZNA (wymagania minimalne)**	
1.	**KOMPUTER STACJONARNY**	**18 szt.**
	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna, stacja graficzna.
	Procesor	Procesor wielordzeniowy oraz wielowątkowy osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 19500 pkt. według wyników procesorów publikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Na potwierdzenie spełniania wymogu Wykonawca dostarczy wraz z ofertą sprzętu wydruk ze strony potwierdzający uzyskanie żądanego wyniku. Wydruk musi być wykonany na dzień przypadający w okresie od ogłoszenia postępowania do dnia otwarcia ofert.
	Pamięć RAM	16GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB. Jeden sloty DIMM wolny.
	Pamięć masowa	512 GB SSD M.2 PCIe NVMe. Pamięć masowa oferowanego komputera musi posiadać partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego na komputerze po awarii.
	Wydajność grafiki	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Obsługująca funkcje: DirectX 12, OpenGL 4.5. FHD 1920x1080
	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną.
	Napęd optyczny	Wbudowany DVD+/-RW
	Czytnik kart pamięci	na przednim panelu obudowy
	Port słuchawkowo-mikrofonowy	na przednim panelu obudowy
	Karta sieciowa RJ-45	LAN 10/100/1000 Mbps zintegrowana z płytą główną

	Obudowa	Typu Tower Możliwość instalacji minimum dwóch dysków, w tym co najmniej jednego 2,5” i jednego 3,5”. Obudowa musi umożliwiać beznarzędziowe otwarcie oraz beznarzędziowy demontaż dysku. Zasilacz o mocy min. 260W pracujący w sieci 230V 50/60Hz prądu zmiennego. Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED przycisku POWER (tzn. barw i miganie) W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, uszkodzenie kontrolera video, awarię CMOS baterii, awarię BIOS’u, awarię procesora. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. Wbudowane porty i złącza: 1 szt. HDMI 1 szt. DisplayPort 4 porty USB na przednim panelu obudowy (w tym min. 2 porty USB 3.0) i min. 4 porty USB na tylnym panelu obudowy (w tym min. 2 porty USB 3.0) wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.; port słuchawkowo-mikrofonowy oraz czytnik kart na przednim panelu, Porty wewnętrzne wolne: PCI-e16 – 1 szt. PCI-e x 1 – 2 szt. SATA III – 1 szt. Kieszeń wewnętrzna 3,5”/2,5” – 1 szt.
	Klawiatura	USB, w układzie polskim programisty
	Mysz	USB, wyposażona co najmniej w: - przyciski min. 3, - scroll
	Bezpieczeństwo	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.
	BIOS	BIOS zgodny ze specyfikacją UEFI, zawierający logo lub nazwę producenta lub nazwę modelu oferowanego komputera, Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: • wersji BIOS, • numerze seryjnym i dacie wyprodukowania komputera, • włączonej lub wyłączonej funkcji aktualizacji BIOS • ilości i prędkości zainstalowanej pamięci RAM, oraz sposobie obsadzeniu slotów pamięci • typie, prędkości oraz wielkości z pamięci cache L2 i L3 zainstalowanego procesora • pojemności zainstalowanego lub zainstalowanych dysków twardych wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA oraz M SATA

	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional PL lub Windows 11 Professional PL, klucz licencyjny Windows musi być zapisany trwale w BIOS. Zamawiający wymaga fabrycznie nowego systemu operacyjnego nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu. Zamawiający wymaga aby oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności, na przykład z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) stosowanymi przez producenta sprzętu lub inną formą uwiarygodniania oryginalności wymaganą przez producenta oprogramowania stosowną w zależności od dostarczanej wersji. *Opis równoważności:* Zainstalowany system operacyjny spełniający poniższe wymagania: • Licencja bez ograniczeń czasowych. • Polska wersja językowa • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. • Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory wdrożoną u Zamawiającego. • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW. • Internetowa aktualizacja zapewniona w języku polskim. • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim. • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.

		• Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0, 3.0, 4.0, 4,8 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. • Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • 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. • Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. • Graficzne środowisko instalacji i konfiguracji. • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. • Udostępnianie modemu. • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • Możliwość przywracania plików systemowych. • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). • Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit.
	Certyfikaty i standardy	- Certyfikat ISO9001 dla producenta sprzętu - Certyfikat ISO50001 dla producenta sprzętu - Deklaracja zgodności CE Załączyć do oferty.
	Wsparcie techniczne producenta	Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.

2.	**MONITOR**	**18 szt.**
	W ofercie wymagane jest podanie modelu, symbolu oraz producenta.	
	wielkość ekranu	23,8''
	matryca	IPS matowa
	Podświetlenie	LED
	rozdzielczość	1920 x 1080 (FullHD)
	Format obrazu	16:9
	Wielkość plamki	0,275
	wyjście słuchawkowe/wejście mikrofonowe	wbudowane
	Liczba wyświetlanych kolorów	16,7 mln
	Kontrast	1000:1
	Czas reakcji	5 ms
	głośniki	wbudowane
	złącza:	1 szt. HDMI 1 szt. DisplayPort 1 szt. VGA (D-sub) 1 szt. wyjście słuchawkowe 1 szt. wejście audio
	Kąt widzenia pion/poziom	178/178 stopni
	Regulacja kąta pochylenia	TAK
	Możliwość montażu na ścianie	TAK
	Technologia ochrony oczu	Redukcja migotania, redukcja niebieskiego światła
	Dołączone wyposażenie:	1 szt. kabel zasilający 1 szt. kabel HDMI długość 2m

3.	**KOMPUTER PRZENOŚNY**	**5 szt.**
	Typ	Komputer przenośny/laptop. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna, stacja graficzna
	Wielkość matrycy	15,6''
	Powłoka matrycy	Matowa o rozdzielczości FHD 1920x1080
	Procesor	Procesor wielordzeniowy oraz wielowątkowy osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 10400 pkt. według wyników procesorów publikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Na potwierdzenie spełniania wymogu Wykonawca dostarczy wraz z ofertą sprzętu wydruk ze strony potwierdzający uzyskanie żądanego wyniku. Wydruk musi być wykonany na dzień przypadający w okresie od ogłoszenia postępowania do dnia otwarcia ofert.
	Pamięć RAM	16GB DDR4 2666MHz. Możliwość rozbudowy do min 32GB. Jeden slot DIMM wolny.
	Pamięć masowa	512 GB SSD M.2 PCIe NVMe. Pamięć masowa oferowanego komputera musi posiadać partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego na komputerze po awarii.
	Wydajność grafiki	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Obsługująca funkcje: DirectX 12, OpenGL 4.5. FHD 1920x1080
	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną Wbudowane głośniki Wbudowany mikrofon
	Kamera	wbudowana 1mpix
	Touchpad	wbudowany
	Czytnik kart pamięci	wbudowany
	Port słuchawkowo-mikrofonowy	wbudowany
	Karta sieciowa RJ-45	LAN 10/100/1000 Mbps zintegrowana z płytą główną
	Wifi	wbudowany Wi-Fi 5
	Bluetooth	wbudowany moduł
	Klawiatura	wbudowana klawiatura układ polski programisty wraz z wbudowaną wydzieloną klawiaturą numeryczną

	Wbudowane złącza:	3 szt. - USB (w tym USB 3.2 Gen. 1 – 1 szt.) 1 szt. - HDMI 1 szt. – wyjście słuchawkowe/wejście mikrofonowe 1 szt. – czytnik linii papilarnych 1 szt. – gniazdo blokady bezpieczeństwa
	Bateria	3-komorowa 41Wh
	Mysz	Bezprzewodowa USB wyposażona co najmniej w: - przyciski min. 3, - scroll
	Torba	Torba transportowa, usztywniona, zabezpieczająca przed uszkodzeniami, wielofunkcyjna, umożliwiająca transport oferowanego komputera przenośnego oraz pozostałych akcesoriów (zasilacz, mysz USB itp.). Dostosowana do wymiarów zaoferowanego laptopa. Kolor czarny.
	Dołączone wyposażenie:	Zasilacz i kabel zasilający
	Bezpieczeństwo	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.
	BIOS	BIOS zgodny ze specyfikacją UEFI, zawierający logo lub nazwę producenta lub nazwę modelu oferowanego komputera, Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: • wersji BIOS, • numerze seryjnym i dacie wyprodukowania komputera, • włączonej lub wyłączonej funkcji aktualizacji BIOS • ilości i prędkości zainstalowanej pamięci RAM, oraz sposobie obsadzeniu slotów pamięci • typie, prędkości oraz wielkości z pamięci cache L2 i L3 zainstalowanego procesora • pojemności zainstalowanego lub zainstalowanych dysków twardych wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA oraz M SATA
	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional PL lub Windows 11 Professional PL, klucz licencyjny Windows musi być zapisany trwale w BIOS. Zamawiający wymaga fabrycznie nowego systemu operacyjnego nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu. Zamawiający wymaga aby oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności, na przykład z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) stosowanymi przez producenta sprzętu lub inną formą uwiarygodniania oryginalności wymaganą przez producenta oprogramowania stosowną w zależności od dostarczanej wersji.

		Opis równoważności: Zainstalowany system operacyjny spełniający poniższe wymagania: • Licencja bez ograniczeń czasowych. • Polska wersja językowa • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. • Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory wdrożoną u Zamawiającego. • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW. • Internetowa aktualizacja zapewniona w języku polskim. • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim. • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. • Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0, 3.0, 4.0, 4,8 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach.

		• Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • 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. • Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. • Graficzne środowisko instalacji i konfiguracji. • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. • Udostępnianie modemu. • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • Możliwość przywracania plików systemowych. • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). • Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit.
	Certyfikaty i standardy	- Certyfikat ISO9001 dla producenta sprzętu - Certyfikat ISO50001 dla producenta sprzętu - Deklaracja zgodności CE Załączyć do oferty.
	Wsparcie techniczne producenta	Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.

4.	**PAKIET BIUROWY**	**23 szt.**
	Nazwa komponentu	**Wymagane graniczne parametry techniczne**
	Oprogramowanie biurowe	**Microsoft Office Home & Business 2019 PL lub wyższa wersja** **Licencja wieczysta** *Opis równoważności:* - Licencja bez ograniczeń czasowych. - Polska wersja językowa - *Możliwość przeniesienie pakietu biurowego na inny komputer* Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.: – edytor tekstów; – arkusz kalkulacyjny; – narzędzie do przygotowania i prowadzenia prezentacji; – narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami); – pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. – powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem musi odbywać się w języku polskim. – dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego – publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu. – możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). Edytor tekstów musi umożliwiać: – Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. – Wstawianie oraz formatowanie tabel. – Wstawianie oraz formatowanie obiektów graficznych. – Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). – Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. – Automatyczne tworzenie spisów treści. – Formatowanie nagłówków i stopek stron. – Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. – Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. – Określenie układu strony (pionowa/pozioma). – Wydruk dokumentów. – Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. – Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać: – Tworzenie raportów tabelarycznych – Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych

		– Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. – Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) – Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. – Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych – Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych – Wyszukiwanie i zamianę danych – Wykonywanie analiz danych przy użyciu formatowania warunkowego – Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie – Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności – Formatowanie czasu, daty i wartości finansowych z polskim formatem – Zapis wielu arkuszy kalkulacyjnych w jednym pliku. – Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: – Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego – Drukowanie w formacie umożliwiającym robienie notatek – Zapisanie, jako prezentacja tylko do odczytu – Nagrywanie narracji i dołączanie jej do prezentacji – Opatrywanie slajdów notatkami dla prezentera – Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo – Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego – Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym – Możliwość tworzenia animacji obiektów i całych slajdów – Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: – Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, – Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, – Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, – Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, – Automatyczne grupowanie poczty o tym samym tytule, – Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, – Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, – Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, – Zarządzanie kalendarzem, – Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, – Przeglądanie kalendarza innych użytkowników,

		– Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, – Zarządzanie listą zadań, – Zlecanie zadań innym użytkownikom, - – Zarządzanie listą kontaktów, - – Udostępnianie listy kontaktów innym użytkownikom, – Przeglądanie listy kontaktów innych użytkowników, – Możliwość przesyłania kontaktów innym użytkownikom.

5.	**OPROGRAMOWANIE SERWEROWE**
1)	**Windows Server 2022 Standard 16 core** **3 szt.** *Opis równoważności:* Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory, które jest aktualnie wykorzystywane. Licencje zostaną wykorzystane do modernizacji aktualnie posiadanych serwerów w urzędzie. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski. - Licencja bez ograniczeń czasowych. - Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer. - instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym; - w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wieloprocesorowym; - obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu; - praca w roli klienta domeny Microsoft Active Directory; - zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022; - zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP); - zawarta możliwość uruchomienia roli serwera DNS; - zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP); - zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory; - zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory; - zawarta możliwość uruchomienia roli serwera stron WWW; - zawarta funkcjonalność szyfrowania dysków; - dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera; - w ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera; - w ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
2)	**Windows Server 2022 user CALL** **70 szt.** Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 z wdrożoną rolą Active Directory.

II część dostawa i montaż UTM	
Lp.	**SPECYFIKACJA TECHNICZNA (wymagania minimalne)**

	UTM	**1 szt.**
	Wymagania Ogólne	1. 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 mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. 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. 4. 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 – 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. 5. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
	Interfejsy, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum poniższą liczbą i rodzajem interfejsów: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps. 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 system 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.
	Wydajność	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.

		3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 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 2.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.
	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. 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. **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. 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 musi posiadać 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 musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Musi istnieć możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

		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. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
	Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • 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, 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. • 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 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 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 musi dostarczyć oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie musi zapewniać 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 filtrowanie 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 musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN powinny wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). 3. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
	Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. 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. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Musi istnieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Musi istnieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
	Ochrona przed atakami	1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera 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). 7. Musi istnieć możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Musi istnieć możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji musi 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 sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Musi istnieć możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System musi dać 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 musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW muszą 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 np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalać definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dać 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 musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja 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. System musi dać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego 3. Rozwiązanie musi umożliwiać 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. Musi 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 umożliwia 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 Firewall 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. 8. Musi istnieć możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Musi istnieć możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
	Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) na dysku lokalnym lub umożliwiać użycie zewnętrznego nośnika danych do celów logowania i raportowania/ 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 musi zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. 3. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 5. Możliwość włączenia logowania per reguła w polityce firewall.

		6. Musi istnieć możliwość logowania do serwera SYSLOG. 7. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
	Obudowa	Musi istnieć możliwość instalacji UTM w szafie RACK 19”
	Serwisy i 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 minimum 24 miesiące.
	Gwarancja oraz wsparcie	Gwarancja polegająca 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. <u>Uwaga: przy zwiększeniu czasu gwarancji należy wydłużyć o ten sam czas: serwisy i licencje.</u>
	Szkolenie	1. Szkolenie zaawansowane z oferowanego systemu, odbędzie się w siedzibie Zamawiającego: 2. Czas szkolenia min. 6h. 3. Liczba osób do przeszkolenia: 3
	Montaż i wdrożenie	1. Wdrożenie zgodnie z wytycznymi klienta 2. Przełączenie produkcyjne 3. Testy po uruchomieniu

III część dostawa i montaż zbiorczego UPS		
Lp.	**SPECYFIKACJA TECHNICZNA (wymagania minimalne)**	
	UPS **1 szt.**	
	W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do: 1. dostawy i montażu zbiorczego UPS wraz z akumulatorami (wraz z niezbędnym okablowaniem) w siedzibie Zamawiającego, 2. wpięcia dostarczonego urządzenia w sieć energetyczną Zamawiającego - (podłączenie do: Zamawiający posiada zewnętrzny bypass oraz zewnętrzny przycisk bezpieczeństwa do wyłączenie UPS (wyłącznik ppoż.) 3. uruchomienia dostarczonego UPS, 4. zagospodarowania odpadów pozostałych po wykonaniu wymiany urządzenia, w tym UPS Cover Partner 15kVA i akumulatorów oraz ich utylizacji zgodnie z obowiązującymi w tym zakresie przepisami, 5. przeszkolenia pracowników urzędu z obsługi UPS: a) zasady wykonywania podstawowych czynności operatorskich (włączanie, wyłączenie, wyłączenie awaryjne) b) właściwa interpretacja informacji sygnalizowanych przez urządzenie c) podstawowe zasady diagnostyki stanów awaryjnych d) zasady postępowania w sytuacjach awaryjnych e) podstawowe zasady BHP przy obsłudze urządzenia 6. wykonania bezpłatnych przeglądów serwisowych w ramach gwarancji i rękojmi raz na 12 miesięcy, 7. możliwość sprawdzenia miejsca instalacji i sieci elektrycznej Zamawiającego, po uprzednim uzgodnieniu telefonicznym, 8. wykonanie pracy zostanie dokonane po podpisaniu protokołu odbioru przedmiotu zamówienia przez Wykonawcę, Zamawiającego oraz inspektora nadzoru.	
	zbiorczy UPS	15kVA/15kW
	ilość faz wejście/wyjście	3 fazowy/3 fazowy
	czas pracy przy pełnym obciążeniu	**15 minut**
	czas przełączania w tryb awaryjny	zerowy czas
	Parametry wejściowe:	
	napięcie znamionowe	380/400/415VAC
	częstotliwość znamionowa	50/60Hz
	THDi	<3% dla 100% obciążenia
	współczynnik mocy	> 0.99
	Bypass:	
	napięcie znamionowe	380/400/415VAC
	częstotliwość znamionowa	50/60Hz
	Parametry wyjściowe:	
	napięcie znamionowe	380/400/415VAC
	częstotliwość znamionowa	50/60Hz
	współczynnik mocy	1
	stabilizacja napięcia	+- 1% (0-100% obciążenia liniowego)

	współczynnik mocy	1
	THDu	<1% (obciążenie liniowe) <4% (obciążenie nie-liniowe) zgodnie z IEC/EN62040-3
	przeciążenie	102% ciągłe 110% 60 min 125% 10 min 150% 1 min >150% 200ms
	akumulatory	AGM hermetyczne, bezobsługowe o żywotności 10-12 lat wg klasyfikacji EUROBAT
	porty komunikacyjne	SNMP, RS-232, USB
	wyświetlacz LCD	TAK w języku polskim
	zabezpieczenia przeciwprzepięciowe, przeciążeniowe i zwarciowe	TAK
	obudowa	UPS oraz zespół bateryjny na kółkach, z blokadą przemieszczania
	wymiary UPS	maksymalne wymiary UPS wraz z akumulatorami: szerokość 110 cm, głębokość 80 cm, wysokość 140 cm
	Panel zdalny	TAK, montowany na I piętrze Uwaga do instalacji: położony kabel łączący posiadany panel zdalny do starego UPS
	Głośność	<56dB
	Montaż	Na poziomie -1 (10 schodów), możliwość wjechania wózkiem przez drzwi garażowe spadek – 20%
	Monitoring pracy przez sieć	Karta SNMP do zdalnego monitoringu pracy przez sieć
	Oprogramowanie	do zarządzania UPS, oraz możliwością ustalenia czasu wyłączenia komputerów przy pracy bateryjnej, automatyczne wyłączenie serwerów (wirtualizacja)
	Rozbudowa	Możliwość rozbudowy do min. 25kV (zmiana miejsca instalacji, bez limitu wymiarów)
	Współpraca z agregatem prądotwórczym	TAK
	Sprawność	Tryb normalny: ≥ 95% Tryb bateryjny: ≥ 95% Tryb Eco: ≥ 99%
	Parametry środowiskowe:	
	Temperatura pracy	Od 0 °C do +40°C
	Wilgotność względna	0-95% (bez kondensacji)
	Certyfikaty	ISO 9001 Deklaracja zgodności CE Dołączyć do oferty.

	Przeglądy serwisowe: wykonania bezpłatnych przeglądów serwisowych w ramach gwarancji i rękojmi raz na 12 miesięcy	Min. 2 w ramach 24 miesięcznej gwarancji
	Dokumentacja powykonawcza:	- karta katalogowa - instrukcja obsługi - karta gwarancyjna - deklarację zgodności - skrócona instrukcja przełączeń - pomiary skuteczności ochrony przeciwporażeniowej - pomiary z pracy UPS'a, pracy bateryjnej

❖ Wykonawca zobowiązany jest dołączyć do formularza ofertowego zestawienie zawierające zaproponowaną konfigurację sprzętu komputerowego oraz UPS, producenta, markę i model, ze szczególnym uwzględnieniem poszczególnych parametrów.

❖ Rękojmia i gwarancja:

1. Na przedmiot zamówienia Wykonawca udzieli..... gwarancji i rękojmi.
   Bieg terminu gwarancji liczony będzie od dnia sporządzenia protokołu odbioru przedmiotu umowy podpisanego przez upoważnionych przedstawicieli stron.
2. W okresie gwarancyjnym Wykonawca zobowiązany jest do bezpłatnej naprawy przedmiotu zamówienia lub wymiany na nowy wolny od wad w przypadku braku możliwości naprawy uszkodzonego sprzętu komputerowego/UPS/oprogramowania.

3*) Część I, Część III Wykonawca oświadcza, że w przypadku ujawnienia wad sprzętu komputerowego/UPS w okresie gwarancji i rękojmi przystąpi do usunięcia wad w terminie do 72 h od momentu otrzymania od Zamawiającego zgłoszenia.

3*) Część II Gwarancja polegająca 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.

4. W przypadku awarii dysków twardych zamontowanych w komputerach, uszkodzony dysk pozostaje u Zamawiającego.
5. Zamawiający może dochodzić roszczeń z tytułu gwarancji i rękojmi za wady także po terminie określonym w §5 ust. 1, jeżeli zgłoszenie wady nastąpiło przed upływem tego terminu.
6. Jeżeli z jakiegokolwiek powodu Wykonawca nie usunie wady (usterki) w wyznaczonym terminie, Zamawiający ma prawo bez upoważnienia Sądu polecić usunięcie takiej wady (usterki) osobie trzeciej, a Wykonawca zobowiązany jest pokryć związane z tym koszty w ciągu 14 dni licząc od daty otrzymania dokumentu zapłaty. Przed powierzeniem wykonania zastępczego innej osobie, Zamawiający wyznaczy Wykonawcy dodatkowy termin na usunięcie wady lub usterki.