



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 4 do zapytania ofertowego

Opis przedmiotu zamówienia

do postępowania o udzielenie zamówienia publicznego na zadanie pod nazwą:

„Dostawa sprzętu i oprogramowania oraz realizacja szkoleń”

w ramach realizacji projektu „Cyfrowa Gmina”

Projekt „Cyfrowa gmina” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020, pakiet REACT-UE.

Część I

Dostarczony sprzęt powinien być:

- fabrycznie nowy, wyprodukowany nie wcześniej niż w 2022 r.
- wyposażony we wszelkie komponenty zapewniające właściwą instalację i użytkowanie (np. akumulatory, przewody zasilające itp.)

W poniższej tabeli zamieszczono **minimalne wymagania** jakie powinna spełniać oferta Wykonawcy:

1. Stacje robocze All-in-One szt. 9

Wymagane minimalne parametry techniczne	
Procesor	- obsługujący funkcje karty grafiki, - przynajmniej 4-rdzeniowy, 8-wątkowy o częstotliwości bazowej 3,7GHz - Osiągający w teście Passmark CPU Mark średni wynik przynajmniej 8650. Do oferty należy dołączyć wydruk ze strony: https://www.cpubenchmark.net/high_end_cpus.html lub http://www.cpubenchmark.net/mid_range_cpus.html
Wydajność obliczeniowa	Komputer w oferowanej konfiguracji musi osiągać łącznie w testach wydajnościowych wyniki nie gorsze niż:



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	Bapco SysMark 25: Overall – min. 1000 punktów Bapco SysMark 25: Productivity– min. 1080 punktów Bapco SysMark 25: Creativity – min. 1090 punktów Bapco SysMark 25: Responsiveness– min. 700 punktów Test musi być przeprowadzony dla automatycznej konfiguracji oprogramowania testującego BAPCO SysMark oraz przy włączonych wszystkich urządzeniach. Test musi być przeprowadzony dla minimum trzech iteracji. Dla każdej przeprowadzanej iteracji muszą zostać osiągnięte wyniki wskazane powyżej. Wymagane testy wydajnościowe muszą być przeprowadzone na automatycznych ustawieniach konfiguratora dołączonego przez BAPCO i przy włączonych wszystkich urządzeniach. Nie dopuszcza się stosowanie overclockingu, 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.).
Płyta główna	- Współpracująca z oferowanym procesorem; - Chipset rekomendowany przez producenta procesora. Obsługująca pamięci typu DDR4. - Wymagane gniazda kart rozszerzeń i napędów: - 2 złącza pamięci DDR4 (obsługa minimum do 32GB RAM), - 2 złącza M.2 - 1 złącza SATA Wymienione gniazda nie mogą być uzyskane w wyniku zastosowania konwerterów lub przejściówek.
Porty wejścia / wyjścia	- Komputer musi posiadać następujące zewnętrzne gniazda wejścia/wyjścia: 1 gniazdo HDMI, 1 gniazdo D-SUB 6 gniazd USB (w tym minimum 4 w standardzie USB 3.1 i minimum 2 gniazda wyprowadzone w dyskretny sposób z boku monitora – niewidoczne z przodu), 1 gniazdo LAN, 2 gniazda Audio,
Pamięć RAM	Min. 8GB DDR4
Dysk twardy	Min. 256GB w technologii SSD PCIe M.2



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Karta Grafiki:	- Zintegrowana z procesorem - Fabrycznie podłączona do monitora sygnałem cyfrowym. Posiadająca dodatkowe wyjścia min. HDMI i D-SUB. - Wymagana obsługa DirectX co najmniej w wersji 12.
Karta dźwiękowa	- Zintegrowana z urządzeniem, zgodna z High Definition Audio.
Karta sieciowa	- Interfejs wbudowany w obudowę lub płytę główną. - minimum 1 x 10/100/1000 Mbps (RJ-45, Gigabit Ethernet). - Wi-Fi 802.11 ac, Bluetooth.
Obudowa	- Obudowa typu All-In-One. Kolor czarny. - Wymiary maksymalne ekranu (nie licząc podstawy i stopy) nie większe niż 542mm x 324mm x 50mm. - Przyciski Power i Reset wyprowadzone z boku lub od spodu monitora. - Matryca typu LED IPS o rozmiarze 23,8 cala, o kącie widzenia min 178 x 178 stopni. Matowa powierzchnia ekranu. Rozdzielczość min. 1920 x 1080 Full HD. 250 nit (cd/m2), liczba wyświetlanych kolorów 16,7 mln, regulacja cyfrowa (OSD), - Ergonomiczna stopa zapewniająca pełną regulację (wysokość, kont nachylenia, pivot, obrót). - Kompatybilność VESA 100 x 100 mm - Obudowa fabrycznie wyposażona w kamerę FHD (z możliwością fizycznego ukrycia), - wbudowany mikrofon oraz głośniki stereo,
Zasilanie	- O mocy minimum 120W, dostosowany do wymagań oferowanej konfiguracji. - Przystosowany do pracy w sieci 230V, 50Hz, - zewnętrzny lub zintegrowany w obudowie.
Klawiatura	Klawiatura USB w układzie polski programisty - trwale oznaczona logo producenta jednostki centralnej
Mysz	Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) - trwale oznaczona logo producenta jednostki centralnej + podkładka pod mysz
System operacyjny	System operacyjny klasy PC nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zaporę internetową (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 multimedialny, pomoc, komunikaty



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

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 służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.

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.

Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.

Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.

Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.

Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.

Wbudowany system pomocy w języku polskim;

Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;

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 2.0 , 3.0 , 3.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;

Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;

Graficzne środowisko instalacji i konfiguracji;

Transakcyjny system plików pozwalający na stosowanie przydziałów 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



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	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). Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu Na dysku twardym dedykowana partycja umożliwiająca szybkie odtworzenie fabrycznie skonfigurowanej wersji systemu (Recovery). Licencja systemu operacyjnego musi pochodzić z oficjalnego kanału dystrybucyjnego w Polsce, musi być nowa, a klucz nigdy wcześniej nie wykorzystywany ani aktywowany.
Gwarancja i Serwis	Gwarancja producenta 24 miesiące w systemie door to door. Czas skutecznej naprawy uszkodzonego sprzętu max. 6 dni roboczych. W przypadku usterki dysku twardego pozostaje on u Zamawiającego. Serwis świadczony przez producenta sprzętu lub przez firmę posiadającą autoryzację producenta. Firma serwisowa świadcząca usługi serwisowe musi spełniać normę ISO 9001. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – załączyć do oferty
Dodatkowe wymagania:	- Deklaracja CE / UE – załączyć do oferty - Certyfikaty jakości producenta - ISO 9001, ISO 14001, ISO 27001, ISO 50001 – załączyć do oferty - Głośność jednostki mierzona według normy ISO 9296/7779 ma wynosić maksymalnie 24 dB (praca w trybie IDLE). Test przeprowadzony na konfiguracji ofertowanej. Należy przedstawić raport z testów wykonanych przez niezależną jednostkę badawczą – załączyć do oferty

2. Komputery przenośne szt. 3

Wymagane minimalne parametry techniczne	
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED matryca matowa
Procesor	Procesor osiągający wynik min. 6040 punktów w teście PassMark CPU Mark według wyników ze strony https://www.cpubenchmark.net/cpu_list.php , na dzień nie wcześniej niż dzień ogłoszenia postępowania.
Pamięć RAM	8GB DDR4 możliwość rozbudowy do min 16GB
Pamięć masowa	min. 256 GB SSD PCIe NVMe, fabryczna możliwość instalacji drugiego dysku 2,5"
Karta graficzna	Zintegrowana z procesorem
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy min. 2x 1W, cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze.
Bateria i zasilanie	Bateria min. 40 WHr. Bateria z funkcją szybkiego ładowania. Zasilacz o mocy min. 65W
Waga	Waga komputera z baterią nie większa niż 2kg
Obudowa	Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z wzmocnianego metalu.
BIOS	BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy. BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej. Funkcja blokowania/odblokowania portów USB Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS'u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł/wy funkcji. Możliwość przypisania w BIOS numeru nadawanego przez Administratora.
Bezpieczeństwo	System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego. Dedykowany układ szyfrujący TPM 2.0
Certyfikaty	Certyfikat ISO 9001 dla producenta sprzętu - załączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu - załączyć do oferty Deklaracja zgodności CE - załączyć do oferty



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

System operacyjny	System operacyjny klasy PC nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zaporę internetową (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 multimedialny, 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 służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 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. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Wbudowany system pomocy w języku polskim; Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
-------------------	--



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	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 2.0 , 3.0 , 3.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Graficzne środowisko instalacji i konfiguracji; Transakcyjny system plików pozwalający na stosowanie przydziałów 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 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). Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu Na dysku twardym dedykowana partycja umożliwiająca szybkie odtworzenie fabrycznie skonfigurowanej wersji systemu (Recovery). Licencja systemu operacyjnego musi pochodzić z oficjalnego kanału dystrybucyjnego w Polsce, musi być nowa, a klucz nigdy wcześniej nie wykorzystywany ani aktywowany.
Wymagania dodatkowe	Wbudowane porty i złącza: HDMI 1.4, RJ-45 (10/100/1000), min. 3xUSB w tym min. 2 port USB 3.2, czytnik kart SD, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, slot zabezpieczający. Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11ac, moduł bluetooth Klawiatura podświetlana (układ US -QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z obsługą gestów.
Warunki gwarancji	2-letnia gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów. Firma serwisująca musi posiadać ISO 9001: 2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

3. Komputery przenośny szt. 1

Wymagane minimalne parametry techniczne	
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej.
Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości 2560 x 1440 z podświetleniem LED, matryca matowa IPS 165Hz.
Wydajność	Procesor osiągający wynik min. 23000 punktów w teście PassMark CPU Mark według wyników ze strony https://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	32GB DDR5 Komputer wyposażony w minimum dwa banki pamięci umożliwiające pracę w trybie dual-channel.
Pamięć masowa	512GB SSD M.2 PCIe NVMe
Karta graficzna	Zewnętrzna karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 18000 punktów w Average G3D Mark, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki o średniej mocy 2 x 2W, dwa cyfrowe mikrofony wbudowane w obudowę matrycy. Kamera internetowa o rozdzielczości min. 1080p trwale zainstalowana w obudowie matrycy, z przestroną obiektywem.
Bateria i zasilanie	Bateria min. 78 WHr, umożliwiająca jej szybkie naładowanie do 70% w czasie 30 minut Zasilacz o mocy min. 280W
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane. Częściowo wykonana z aluminium.
Waga	Waga komputera z baterią nie większa niż 2,5kg
BIOS	BIOS zgodny ze specyfikacją UEFI
Bezpieczeństwo	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	Certyfikat ISO 9001: 2000 dla producenta sprzętu – załączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu – załączyć do oferty



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	Deklaracja zgodności CE – załączyć do oferty
Wymagania dodatkowe	Wbudowane porty i złącza: HDMI, RJ-45 (100/1000), min. 3 x USB 3.2, 3 x USB 3.2 typ C, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania Zintegrowana w postaci wewnętrznego modułu karta sieci WLAN 802.11AX, moduł bluetooth 5.1. Klawiatura (układ US-QWERTY) podświetlana z wydzieloną klawiaturą numeryczną, touchpad wraz z obsługą gestów.
System operacyjny	System operacyjny klasy PC nie wymagający aktywacji za pomocą telefonu lub Internetu, spełniający następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zaporę internetową (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 multimedialny, 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 służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 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. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Wbudowany system pomocy w języku polskim; Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 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 2.0 , 3.0 , 3.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Graficzne środowisko instalacji i konfiguracji; Transakcyjny system plików pozwalający na stosowanie przydziałów 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 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). Telefoniczne wsparcie techniczne w języku polskim w dni robocze od 8:00 do 17:00 zapewniony przez producenta lub dostawcę co najmniej przez 5 lat od chwili zakupu Na dysku twardym dedykowana partycja umożliwiająca szybkie odtworzenie fabrycznie skonfigurowanej wersji systemu (Recovery). Licencja systemu operacyjnego musi pochodzić z oficjalnego kanału dystrybucyjnego w Polsce, musi być nowa, a klucz nigdy wcześniej nie wykorzystywany ani aktywowany.
Warunki gwarancji	2-letnia gwarancja producenta

4. Oprogramowanie biurowe szt. 13



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Wymagane minimalne parametry techniczne

Wymagania dla pakietu biurowego

Pakiet zintegrowanych aplikacji biurowych powinien zawierać:

- Edytor tekstu,
- Arkusz kalkulacyjny,
- Narzędzie do przygotowywania i prowadzenia prezentacji,
- Klient poczty elektronicznej.

Interfejs aplikacji musi być całkowicie w języku polskim.

Do aplikacji musi być dostępna pełna dokumentacja w postaci pomocy dla użytkownika w języku polskim.

Edytor tekstów musi umożliwiać:

- edycję i formatowanie tekstu w języku polskim,
- 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 nagłówek i stopek stron,
- sprawdzanie pisowni w języku polskim,
- śledzenie zmian wprowadzonych przez użytkowników,
- 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,
- pracę na dokumentach zgodnymi w pełni z formatem Microsoft Word 2007,
- zabezpieczenie hasłem dokumentów przed odczytem oraz wprowadzaniem modyfikacji,
- integrację z narzędziami do pracy grupowej.

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),



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
- wyszukiwanie i zamienianie 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,
- pracę na plikach zgodnych w pełni z formatem Microsoft Excel 2007,
- zabezpieczenie hasłem dokumentów przed odczytem oraz wprowadzaniem modyfikacji,
- integrację z narzędziami do pracy grupowej.

Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

- przygotowywanie prezentacji multimedialnych, które będą:
- prezentowane przy użyciu projektora multimedialnego,
- drukowane w formacie umożliwiającym robienie notatek,
- zapisane 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,²
- 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,
- pracę na dokumentach zgodnych w pełni z formatem Microsoft PowerPoint 2007,
- integrację z narzędziami do pracy grupowej

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

- ma zdefiniowany układ informacji w postaci XML

Klient poczty elektronicznej musi umożliwiać:

- zarządzanie Skrzynką Odbiorczą za pomocą Reguł, Kategorii, białych i czarnych list
- zarządzanie Kalendarzem
- zarządzanie Zadaniem



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	- zarządzanie Kontaktami - komunikowanie się za pośrednictwem poczty elektronicznej - obsługiwać usługi POP, IMAP oraz Microsoft Exchange lub zgodne - umożliwiać tworzenie Notatek Oprogramowanie dopuszczone dla użytkownika biznesowego Licencja wieczysta
--	---

5. Urządzenie wielofunkcyjne szt. 1

Wymagane minimalne parametry techniczne	
Wymagane funkcje	Kopiarka, drukarka sieciowa, skaner sieciowy
Technologia druku	technologia laserowa, kolorowa, czterobębnowa
Format oryginału	A4
Format kopii	A4-A6
Prędkość druku	Min. 30/30 stron A4 czarno-białych/kolorowych na minutę.
Obsługiwane rozdzielczości drukowania	600x600 dpi, 1200x1200 dpi
Czas pierwszego wydruku	kolorowego – maks. 8 sek., czarno-białego – maks. 7 sek.
Czas nagrzewania	maks. 30 sek. od włączenia zasilania
Kopiowanie wielokrotne	1- 999 kopii
Pamięć RAM	min. 1 GB (możliwość rozbudowy do min. 3 GB)
Zoom	25-400%
Panel operatora	Panel wyposażony w kolorowy ekran dotykowy LCD (min. 7-calowy), opisy na panelu oraz komunikaty na ekranie w języku polskim, panel z regulowanym położeniem w min. 2 pozycjach.
Dupleks	w standardzie
Podajnik dokumentów	automatyczny – dwustronny na min. 70 ark.
Podajniki papieru	min. 1 kaseta na 250 ark. A5-A4, 60-160 g/m ² ; min. 1 taca uniwersalna na 100 ark. A6-A4, 60-220 g/m ² ;
Funkcja druku sieciowego	w standardzie
Emulacje	PCL 6, PostScript 3, wydruk bezpośredni plików PDF i XPS



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Interfejsy	USB 2.0, Ethernet 10/100/1000Base-T, USB dla pamięci przenośnej, gniazdo pamięci typu SD/SDHC®;
Funkcja skanowania sieciowego	w standardzie, skanowanie pełno-kolorowe
Funkcje skanowania	skanowanie do e-mail, do FTP, do-SMB, TWAIN sieciowy, WSD, do pamięci przenośnej USB
Rozdzielczość skanowania	600 dpi
Prędkość skanowania	Mono: min. 60 str./min., kolor: min. 40 str. / min. (300 dpi/A4)
Typy plików	PDF, PDF/A, PDF szyfrowany, PDF skompresowany, PDF przeszukiwalny, JPEG, TIFF, XPS, MS Office (docx, xlsx, pptx)
Możliwość rozbudowy	• Podajniki papieru o pojemności łącznej min. 1500 ark. formatu A4, 80 g/m²; • Karta sieciowa Wireless LAN 802.11b/g/n • Interfejs Direct WiFi • Dysk HDD lub SSD o pojemności min. 120 GB • Zszywacz min. 1-pozycyjny
Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny jednostkowej).	Toner - właściwa ilość, która zapewni wydrukowanie minimum 2 000 stron kolorowych A4 (zgodnie z ISO19798) Bęben - właściwa ilość, która zapewni wydrukowanie minimum 200 000 stron kolorowych A4
Gwarancja	24 miesiące, świadczona przez producenta lub autoryzowany serwis.

6. Oprogramowanie do audytów bezpieczeństwa, kontroli legalności oprogramowania oraz szyfrowania danych zgodnych z KRI szt. 1

Wymagane minimalne parametry techniczne	
Wymagana funkcjonalność oprogramowania zawarta w systemie:	• W pełni webowa konsola zarządzania systemem. • Baza danych pracująca na silniku Microsoft SQL Server • Wspólna baza CMDB dla całości systemu (infrastruktura, procesy, dokumenty, usługi, relacje). • System umożliwia wykorzystanie dowolnej liczby interfejsów sieciowych oraz wdrożenie architektury rozproszonej poprzez wykorzystanie wielu serwerów. • 100 interaktywnych widżetów. Widżety obsługują metodę drill-down i pozwala na pełną konfigurowalność.



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- Ponad 30 interaktywnych widgetów. Obsługa metody drill-down. Wskazuje elementy infrastruktury IT w obszarze bezpieczeństwa IT.
- Spersonalizowany widok pod konkretnego użytkownika systemu (dashboardy, aktywne skróty).
- Automatyczna inwentaryzacja infrastruktury IT w zakresie komputerów stacjonarnych i przenośnych, w sieci jak i poza siecią lokalną, a także serwerów, drukarek, dowolnych urządzeń sieciowych oraz zasobów dodanych manualnie.
- Automatyczna inwentaryzacja systemów operacyjnych, oprogramowania zainstalowanego, oprogramowania portable. Wsparcie dla modeli: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value, CAL, SAAS, Trial, Shareware.
- Zdalne zarządzanie komputerami – ponad 100 predefiniowanych poleceń CMD i PowerShell. Wbudowany harmonogram,
- Zdalne zarządzanie komputerami z wykorzystaniem RDP, VNC, Intel vPro. Zdalne połączenie do komputera w sieci lokalnej do sesji użytkownika. Multi VNC – jednoczesny dostęp do wielu komputerów. Pełne wsparcie dla technologii Intel VPRO/AMT w zakresie konfiguracji BIOS, uruchomienie wyłączonego komputera oraz reinstalację systemu operacyjnego
- Uruchomienie wyłączonego komputera oraz reinstalację systemu operacyjnego
- Automatyczne powiadomienia dotyczące aktualności w konsoli administracyjnej, (wspierane kanały: email, SMS, powiadomienia na pulpicie administratora, powiadomienia użytkownika),
- Zwracanie informacji o obciążeniu procesami, dyskach twardych oraz ruchu sieciowym
- Identyfikowanie sieci lokalnych oraz zbudowanie map sieci (w tym rozległych) oraz udostępnianie szczegółowych informacji o wszystkich urządzeniach sieciowych (obsługę SNMP)
- Monitorowanie drukarek znajdujących się w sieci firmowej. Odczytywanie informacji szczegółowych o drukarkach (poziom tonerów, marginesy, powiadomienia, porty). Możliwość przejścia do panelu zarządzania drukarką.
- Monitorowanie szybkości komunikacji między różnymi typami urządzeń dostępnych w infrastrukturze sieci a serwisami (ponad 30), z których korzystają.
- monitorowanie: logowania, drukowania, stron www, transferu sieciowego, urządzeń USB, usług, procesów, wydajności, dzienników zdarzeń, sesji RDP,
- Monitorowanie procesów, usług oraz wydajności komputerów i serwerów,
- Monitorowanie procesów, usług oraz wydajności komputerów i serwerów (wspiera Hyper-V oraz VMware). Zwraca informację o obciążeniu procesami, dyskach twardych oraz ruchu sieciowym.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	• Prowadzenie ewidencji ilościowo-wartościowej dla akcesoriów i infrastruktury informatycznej. • Klasyfikator stron internetowych / klasyfikator procesów i aplikacji - zaimplementowane klasyfikatory zwracają informację o kategorii, bezpieczeństwie oraz produktywności stron www i uruchamianych procesów / aplikacji, oparte o sztuczną inteligencję w zarządzaniu IT • Zdalne wysyłanie alertów oraz jednorazowych lub cyklicznych wiadomości do użytkowników komputerów. Wiadomości podążają za użytkownikiem. • Możliwość komunikacji administratora IT z użytkownikami, w tym prowadzenie rozmów indywidualnych, grupowych, używanie harmonogramu, wiadomości predefiniowanych, statusy dostarczeni. • System powinien posiadać uwierzytelnianie dwuskładnikowe, jest to dodatkowe zabezpieczenie poświadczeń użytkownika podczas procesu logowania. • Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej. • System musi uniwersalny interfejs programistyczny (API) do widoków tabelarycznych • Szyfrowanie BitLocker (HDD+USB), zdalne masowe szyfrowanie / deszyfrowanie partycji dysków komputerów zewnętrznych i wewnętrznych w sieci lokalnej jak i poza siecią, bieżący status procesu. Identyfikacja partycji zaszyfrowanych, magazynowanie kluczy odzyskiwania. Wsparcie dla metod szyfrowania: AES 128 lub 256-bit. • Automatyczna zdalna instalacja / deinstalacja oprogramowania na jednym lub grupie komputerów. Wsparcie dla wielu repozytoriów. Automatyczny wybór repozytorium na podstawie wyznaczania optymalnej trasy pakietu.
--	---

7. Oprogramowanie domenowe szt. 1

Wymagane minimalne parametry techniczne	
Funkcje oprogramowania	1. System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Warunki licencjonowania systemu operacyjnego muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer. 4. W ramach dostarczonej licencji na system operacyjny musi być zawarta możliwość instalacji oprogramowania na



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	serwerze wieloprocesorowym; - System operacyjny musi mieć możliwość obsługi 64 procesorów fizycznych. - System operacyjny musi obsługiwać pamięć RAM w ramach jednej instancji systemu operacyjnego w wysokości przynajmniej 24TB; - Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat; - System operacyjny musi mieć 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); - Licencja na system operacyjny musi być bez ograniczeń czasowych. - Licencja na system operacyjny musi pozwalać na zainstalowanie systemu przez Zamawiającego na fizycznym serwerze z jednym fizycznym procesorem szesnastordzeniowym zgodnie z polityką licencjonowania producenta oprogramowania. - Licencja musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. - Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. - System operacyjny musi posiadać graficzny interfejs użytkownika. - System operacyjny musi być w pełni kompatybilny z usługą domenową w zakresie: - zarządzania użytkownikami, - zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, - możliwości przydzielania praw dostępu do zasobów sieciowych, - instalacji zdalnej oprogramowania z pakietów MSI, - definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych. - System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. - System operacyjny musi posiadać obsługę zdalnego pulpitu. - System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. - Wszystkie narzędzia i usługi wykorzystywane w systemie operacyjnym powinny być rozwiązaniem jednego producenta. - System operacyjny musi pozwalać na obsługę pamięci USB jako monitora klastra. - System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra.
--	--



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	21. System operacyjny musi posiadać obsługę deduplikacji. 22. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 23. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zaporę musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6. 24. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny; 25. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 26. Liczba licencji dostępowych do serwera liczona w modelu na użytkownika: 25szt. 27. Oprogramowanie nie może być ograniczone czasowo w użytkowaniu 28. Wymagana oprogramowanie w najnowszej wersji dostępnej na rynku.
Oprogramowanie i usługa wdrożeniowa.	a) należy dostarczyć poniżej opisany system operacyjny b) należy zainstalować oprogramowanie na serwerze (w posiadaniu Zamawiającego) oraz wdrożyć usługę dla 25 użytkowników w zakresie: - utworzenie kont, - migracja komputerów do domeny, - utworzenie dysków sieciowych, - utworzenie podziału użytkowników na grupy uprawnień. c) szkolenie administratora z obsługi, min. 2h.

8. Serwer plików NAS szt. 1

Wymagane minimalne parametry techniczne	
Procesor	Czterordzeniowy o taktowaniu co najmniej 2,2GHz np. AMD Ryzen V1500B
Architektura procesora	64-bitowy x86
Koprocesor arytmetyczny	Tak
Obudowa	Rack 2U, szyny montażowe do szafy RACK 19"
Pamięć RAM	16GB UDIMM DDR4, możliwość rozszerzenia pamięci RAM do 64GB
Pamięć flash	5GB
Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6Gb/s Zainstalowane 4szt. dysków o poj. 6TB każdy – dedykowane do pracy w urządzeniach typu NAS



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Interfejsy sieciowe	2 x 2,5GbE (RJ45), możliwość zamontowania dodatkowych portów sieciowych 5 GbE, 10GbE poprzez dołożenie opcjonalnych kart.
Gniazdo PCIe	Gniazdo 1: PCIe Gen 3 x8
Porty USB	2 x USB Typu-C 3.2 Gen 2 (10Gb/s) 2 x USB Typu-A 3.2 Gen 2 (10Gb/s)
Wskaźniki LED	HDD 1-8, Stan, LAN, USB, zasilanie
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity
Funkcja Hot Spare	RAID Hot Spare and Global Hot Spare
Szyfrowanie	Możliwość szyfrowania folderów i wolumenów kluczem AES 256-bit.
Wspierane Systemy Operacyjne	1. Apple Mac OS 10.10 or later 2. Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux 3. IBM AIX 7, Solaris 10 or later UNIX 4. Microsoft Windows 7, 8, and 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019
Stacja monitoringu	Obsługa 24 kamer IP (8 licencji domyślnie).
Protokoły	CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Serwer plików, Manager plików przez WWW, Obsługa plików QPKG, Funkcja Virtual Disk umożliwiaiąca zwiększenie pojemności serwera przy pomocy inicjatora iSCSI, Montowanie obrazów ISO, Klient LDAP, Serwer Syslog, Server VPN, Obsługa kontenerów (LXC, Docker), Funkcja migawek, Migawki (min. 1024)
Wirtualizacja	Certyfikaty: VMware vSphere: VMware ESXi 6.7 & 7.0 (iSCSI), VMware ESXi 6.7 & 7.0 (NFS), VMware ESXi 6.7 & 7.0 (VAAI iSCSI), VMware ESXi 6.7 & 7.0 (VAAI NFS), VMware ESXi 6.7 & 7.0 (Fibre Channel) Microsoft Hyper-V: Windows Server 2019, Citrix XenServer: Citrix Ready 8.x
Zarządzanie dyskami	Skanowanie w poszukiwaniu złych sektorów, odczyt S.M.A.R.T
Język GUI	Polski
Waga	Max. 11 kg (brutto)
System plików	Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
Zasilanie	Redundantne (2x 300W)
Wentylatory	Min. 3 x 60 mm



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Gwarancja i serwis	24 miesiące, realizowanej przez producenta lub autoryzowany serwis.
Konfiguracja	- założenie kont użytkowników i nadanie uprawnień - ustawienie dostępu użytkownikom do zasobów macierzy - ustawienie backupu z serwerów/maszyn wirtualnych.

9. Switch szt. 1

Wymagane minimalne parametry techniczne	
	Wymaga się, aby urządzenie jak i zainstalowane zasilacze oraz wentylatory były objęte 24 miesięczną gwarancją producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii. Przełącznik powinien obsługiwać następujące standardy oraz protokoły • IEEE 802.3 10BASE-T • IEEE 802.3u 100BASE-TX • IEEE 802.3ab 1000BASE-T • IEEE 802.3z 1000BASE-X • IEEE 802.3x Porty: • 48 x 10/100/1000 Mb/s Ethernet • 4 x SFP • Automatyczne wykrywanie oraz automatyczna negocjacja parametrów połączenia Wymagane jest aby przełącznik obsługiwał następujące protokoły • IEEE 802.1D • IEEE 802.1W • IEEE 802.1S • Auto-voice VLAN • SNMP v1, v2c, v3 • RFC 1213 MIB II • RFC 1643 Ethernet Interface MIB • RFC1493 Bridge MIB



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

- Jumbo Frame
- IEEE 802.1Q Tag VLAN
- 128 Static VLANs
- IEEE 802.1p
- DSCP - L3 QoS
- Ograniczanie pasma na wejściu
- IEEE 802.3ad
- DHCP client
- Broadcast storm control
- Port mirroring (many-to-one)
- Port setting
- IGMP snooping v1/v2
- IEEE 802.1x (RAIDUS)
- ACL - MAC, IP
- SNTP
- IEEE 802.1ab LLDP
- HTTP and HTTPS
- Ochrona przed DoS
- Syslog
- Ping & traceroute
- Konfiguracja przez www
- IEEE802.3az
- Statyczny routing
- MLD Snooping

Parametry wydajnościowe

- Metoda przesyłania ramek: Store-and-forward
- Przepustowość magistrali: 100 Gb/s
- Wielkość bufora: 2Mb
- Ilość adresów MAC: 16000
- Czas bezawaryjnej pracy przełącznika 390 tys. godzin



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	Przełącznik musi spełniać następujące standardy elektromagnetyczne: • CE mark, commercial • FCC Part 15 Class A • VCCI Class A • EN 55022 (CISPR 22) • EN 55024 (CISPR 24) • UL listed (UL 1950)/cUL • IEC 950/EN 60950 • CE mark, commercial • CUL 60950 (Listed)/EN 60950 (Low Voltage Directive) • Zamawiający wymaga, aby oferowane urządzenia były nowe, nie pochodziły z tzw. odzysku (refurbished). Urządzenia powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta proponowanych urządzeń. Urządzenia powinny być objęte polskim serwisem producenta a ewentualna wymiana gwarancyjna autoryzowana przez polski serwis producenta. • Zamawiający wymaga konfiguracji urządzenia zgodnie z wytycznymi przekazanymi na etapie wdrożenia i konfiguracji pozostałych urządzeń sieciowych (AD, UTM, serwer backupu).
--	---

10. Firewall szt. 1

Wymagane minimalne parametry techniczne	
Należy dostarczyć firewall'a zgodnie z poniższymi wymogami wraz z wdrożeniem obejmującym:	- konfiguracja reguł firewall'a - konfiguracja certyfikatów SSL - inspekcję ruchu HTTPS - konfigurację IPS'a
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



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	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 klastery 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 łącz 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.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	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 - zaporą ogniową 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.



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	• 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.



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	• 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 RIPv2), 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.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	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).



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	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.



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	- 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. - System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. - 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. - Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	- 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. - Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. - Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. - System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. - System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. - Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. - Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. - Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). - Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odp-



Fundusze Europejskie
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	wiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowaniu 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	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 24 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. • Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) – załączyć do oferty • Certyfikat ISO 9001 podmiotu serwisującego – załączyć do oferty
Opisy do wymagań ogólnych	Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym – załączyć do oferty



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Część II

Przeprowadzenie szkoleń pracowników Urzędu Gminy Młodzieszyn pod kątem cyberbezpieczeństwa realizowane w ramach projektu „Cyfrowa Gmina”.

Lokalizacja realizacji zadania :

Siedziba Zamawiającego – Wyszogrodzka 25, 96-512 Młodzieszyn

Czas szkolenia :

Minimalny wymiar czasu – 4 godziny zegarowe na każdą grupę.

Ilość grup szkoleniowych – 2 grupy

Liczba osób w każdej grupie nie przekracza 15 pracowników.

Zakres szkolenia

Szkolenie powinno zawierać tematy z zakresu:

- phishingu (fałszywe maile, podszywanie się, próby wyłudzenia)
- vishingu (telefoniczne i SMS-owe próby wyłudzeń)
- socjotechniki wykorzystywane przez przestępców
- praca z wykorzystaniem nieszyfrowanych połączeń wifi
- malware, ransomware - złośliwe oprogramowanie, szpiegujące, szyfrujące, wymuszające okup
- używanie silnych haseł, różniących się od siebie
- praca z przeglądarką internetową (szyfrowane strony; komunikaty; zapamiętywanie haseł; niepoprawne, podobne adresy stron internetowych)
- posiadanie antywirusa i obserwowanie jego komunikatów
- archiwizacja i szyfrowanie danych
- niezapisywanie haseł przy biurku
- przenoszenie komputera służbowego,

Po zakończeniu szkolenia każdy z uczestników otrzyma imienny certyfikat potwierdzający odbycie szkolenia

Szkolenie odbędzie się stacjonarnie.



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Wykonawca zapewni w cenie szkolenia:

- niezbędne materiały szkoleniowe,
- wydanie certyfikatów ukończenia kursu.

Wraz ze złożoną ofertą, Wykonawca dostarczy referencje oraz agendę szkolenia.