

*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

zał. nr 1.1 do swz

## Opis przedmiotu zamówienia

**Dotyczy: Postępowania o udzielenie zamówienia na: Dostawę, montaż i konfigurację sprzętu komputerowego oraz oprogramowania dla Gminy Majdan Królewski na potrzeby realizacji projektu grantowego „Cyfrowa Gmina”.**

### Minimalne wymagania techniczne:

Zamawiający wymaga zainstalowania całości dostarczonego rozwiązania we wskazanych pomieszczeniach Zamawiającego co najmniej w zakresie:

- Wniesienia, ustawienia i fizycznego montażu wszystkich dostarczonych urządzeń w szafach rack.
- Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać dostarczone w miejsce wskazane przez Zamawiającego, zamontowane, skonfigurowane i uruchomione.
- Usunięcia opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń
- Podłączenia całości rozwiązania do infrastruktury Zamawiającego
- Wykonania procedury aktualizacji firmware dostarczonych elementów środowiska teleinformatycznego do najnowszej stabilnej wersji oferowanej przez producenta sprzętu
- Wykonania połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
- Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające, kable zasilające).



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

## 1 Urządzenie dostępne do pracy zdalnej (1 szt)

### Wymagania ogólne:

Dostarczone urządzenie dostępne do pracy zdalnej musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład urządzenia dostępnego do pracy zdalnej były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Parametr lub warunek	Minimalne wymagania
Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Dysk, Zasilanie	<p>System realizujący funkcję Firewall musi dysponować minimum: 5 portami Gigabit Ethernet RJ-45.</p> <p>System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>W ramach systemu powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System musi być wyposażony w zasilanie AC.</p>



Fundusze Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</p> <p>Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.</p> <p>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 1.4 Gbps.</p> <p>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.</p> <p>9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.</p>
Funkcje Systemu Bezpieczeństwa	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>Kontrola Aplikacji.</p> <p>Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</p> <p>Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.</p> <p>Ochrona przed atakami - Intrusion Prevention System.</p> <p>Kontrola stron WWW.</p> <p>Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</p> <p>Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</p> <p>Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.</p> <p>Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system</p>
Polityki, Firewall	<p>Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <p>Translację jeden do jeden oraz jeden do wielu.</p> <p>Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</p>



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.</p> <p>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.</p> <p>Amazon Web Services (AWS).</p> <p>Microsoft Azure</p> <p>Google Cloud Platform (GCP).</p> <p>OpenStack.</p> <p>VMware NSX.</p>
Połączenia VPN	<p>System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <p>Wsparcie dla IKE v1 oraz v2.</p> <p>Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p> <p>Obsługa protokołu Diffie-Hellman grup 19 i 20.</p> <p>Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.</p> <p>Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</p> <p>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</p> <p>Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</p> <p>System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <p>Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.</p> <p>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</p> <p>Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.</p>
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <p>Routingu statycznego.</p> <p>Policy Based Routingu.</p> <p>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.</p>



Fundusze Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

Funkcje SD-WAN	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencją upoważniającą do korzystania z usługi typu Sandbox w chmurze. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</p>
Kontrola WWW	<p>Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</p> <p>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</p> <p>W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:</p> <p>Hasł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>Hasł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>Hasł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.</p> <p>Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</p>





*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p> <p>System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</p> <p>System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p>
Logowanie	<p>Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p>



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL <sub>4</sub> dla funkcji Firewall.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Rozszerzone wsparcie serwisowe	System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.
Wymagania pozostałe	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego





Fundusze Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
--	---

#### Zestaw 27 szt

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiającą jednoznaczną identyfikację oferowanej konfiguracji. W przypadku wątpliwości co do treści złożonej oferty Zamawiający wezwie wykonawcę do złożenia wyjaśnień w trybie art. 26 ust. 4 lub art. 87 ust. 1 ustawy Prawo zamówień publicznych.
Obudowa	Obudowa o max wymiarach 27 × 9,5 × 30,3 cm i wadze całego rozwiązania nie przekraczająca 3,9 kg
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera umożliwiającą konfigurację wielodyskową min. SATAIII + M.2 PCIe
Procesor	Procesor wielordzeniowy z zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, Intel® Core™ i5-10500 lub równoważny na poziomie wydajności liczonej w punktach na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na <a href="http://www.cpubenchmark.net/">http://www.cpubenchmark.net/</a> . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna	Min. 16 GB DDR4 2666MHz z możliwością rozszerzenia do min 32 GB Ilość banków pamięci: min. 2 szt. Ilość wolnych banków pamięci: min. 1 szt.
Dysk twardy	Min. 512GB SSD M.2 PCIe NVMe oraz zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
Napęd optyczny	Nagrywarka DVD +/-RW
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo 2W, uniwersalne gniazdo jack audio, gniazdo combo - mikrofon/słuchawki



Fundusze  
Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

Porty/złącza	Wbudowane (minimum): Przód: 1 gniazdo combo (słuchawki/mikrofon); 2 porty SuperSpeed USB Type-A o przepustowości 10 Gb/s; 2 porty USB Type-A o przepustowości 480 Mb/s ; Z tyłu: 1 wyjście audio; 1 złącze zasilania; 1 port RJ-45; 1 port HDMI 1.4; 3 porty SuperSpeed USB Type-A o przepustowości 5 Gb/s; 1 port DisplayPort™ 1.4; 2 porty USB Type-A o przepustowości 480 Mb/s
Urządzenia wejściowe	Klawiatura przewodowa + przewodowa mysz optyczna
Karta sieciowa	Port sieci LAN 100/1000 Ethernet RJ 45 zintegrowany z płytą główną. Zainstalowana wewnątrz obudowy bezprzewodowa karta sieciowa dwuzakresowa WiFi AC 2x2 + Bluetooth 5.1
Zasilacz	Energooszczędny wewnętrzny zasilacz o mocy nie większej zasilacz 210 W, sprawność do 92%
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: <ol style="list-style-type: none"> <li>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> <li>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych</li> </ol> </li> <li>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego</li> <li>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim</li> <li>4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.</li> <li>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe</li> <li>6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,</li> <li>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</li> <li>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim</li> <li>9. Wbudowany system pomocy w języku polskim.</li> <li>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</li> </ol>



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24. Wbudowany mechanizm wirtualizacji typu hypervisor."
25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ol style="list-style-type: none"> <li>Login i hasło,</li> <li>Karty inteligentne i certyfikaty (smartcard),</li> <li>Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> <li>Certyfikat/Klucz i PIN</li> <li>Certyfikat/Klucz i uwierzytelnienie biometryczne</li> </ol> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p>
BIOS	<p>Możliwość odczytania z BIOS:</p> <ol style="list-style-type: none"> <li>1. Wersji BIOS wraz z datą wydania wersji</li> </ol>



Fundusze Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3</p> <p>3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności, producencie i obsadzeniu na poszczególnych slotach</p> <p>4. Informacji o dysku twardym: typ, producent, model</p> <p>Możliwość wyłączenia/włączenia: kontrolera audio, portów USB, karty dźwiękowej, wirtualizacji, z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p> <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p> <p>Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora.</p>
Zintegrowany System Diagnostyczny	<p>Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:</p> <p>wykonanie testu pamięci RAM</p> <p>test dysku twardego</p> <p>test monitora</p> <p>test płyty głównej</p> <p>Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregośkolwiek z powyższych podzespołów komputera.</p> <p>Ponadto system powinien umożliwiać identyfikację testowanej jednostki i jej komponentów w następującym zakresie:</p> <p>PC: Producent, model</p> <p>Procesor: Nazwa, taktowanie</p> <p>Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci</p> <p>Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy</p> <p>System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.</p>
Certyfikaty standardy	<p>i</p> <p>Dla producenta sprzętu należy dostarczyć:</p> <p>Certyfikat ISO9001 dla producenta sprzętu</p> <p>Urządzenie musi spełniać:</p> <p>Deklaracja zgodności</p> <p>Certyfikat ENERGY STAR®; Certyfikat EPEAT® 2019</p>
Wirtualizacja	<p>Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej</p>



Fundusze Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
Bezpieczeństwo	Hasło uruchamiania (w systemie BIOS); Wyłączanie portu SATA (w systemie BIOS); Hasło konfiguracji (w systemie BIOS); Obsługa kłódkowego zabezpieczenia obudowy i linek zabezpieczających; Włączanie/wyłączanie portu USB (w systemie BIOS); Włączanie/wyłączanie portu szeregowego (w systemie BIOS); budowany układ zabezpieczający Trusted Platform Module TPM 2.0 dostarczany z systemem
Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
Gwarancja	60 miesięcy świadczona w miejscu użytkowania sprzętu (on-site)
Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego. - możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź





Fundusze  
Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek
--	--



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

### Jednostka Serwerowa 1 KPL

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Typu RACK, wysokość nie więcej niż 2U; Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
Płyta główna	Dwuprocessorowa; Wyprodukowana i zaprojektowana przez producenta serwera 6 aktywnych złącz PCI Express generacji 3 w tym: 3 złącza o prędkości x16 3 złącza o prędkości x8 12 gniazd pamięci RAM; Obsługa minimum 768GB pamięci RAM; Możliwość zainstalowania modułu TPM; Wsparcie dla technologii: Memory Scrubbing SDDC Advanced ECC
Procesory	<ul style="list-style-type: none"> <li>• Procesor 8-rdzeniowy</li> <li>• architektura x86_64</li> <li>• Taktowanie bazowe 2,1GHz</li> </ul> zapewniający wydajność min. 11100 pkt. (dla pojedynczego procesora) w teście Passmark CPU Mark, znajdujący się na liście <a href="https://www.cpubenchmark.net/cpu_list.php">https://www.cpubenchmark.net/cpu_list.php</a> (wynik na dzień 15.06.2022)
Pamięć RAM	<ul style="list-style-type: none"> <li>• Min 64GB pamięci RAM</li> <li>• DDR4 Registered</li> </ul> 2933Mhz
Dyski twarde	<ul style="list-style-type: none"> <li>• Minimum 8 wnęk dla dysków twardych Hotplug 3,5";</li> </ul> Zainstalowane 4 dyski SSD SATA 480GB HOT PLUG 3.5" Zainstalowane 4 dyski SATA 2TB HOT PLUG
Kontrolery LAN	Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI i iSCSI boot;
Kontrolery I/O	Kontroler RAID dla wewnętrznych dysków twardych posiadający obsługujący poziomy RAID: 0,1,10,5,50,6,60 posiadający 2GB pamięci cache
Porty	<ul style="list-style-type: none"> <li>• Zintegrowana karta graficzna ze złączem VGA;</li> <li>• 2 porty USB 3.0 na panelu przednim;</li> <li>• 1 port USB 3.0 wewnętrzny;</li> <li>• 4 porty USB 3.0 dostępne z tyłu serwera;</li> <li>• 1 port serial/RS232 – możliwość rozbudowy;</li> </ul> Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

Zasilanie, chłodzenie	Dwa zasilacze hotplug o sprawności 94% (tzw klasa Platinum) o mocy min 450W, redundancja zasilania; Redundantne wentylatory;
Zarządzanie	<p>Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;</p> <p>Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:</p> <ul style="list-style-type: none"> <li>○ Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;</li> <li>○ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;</li> <li>○ Dostęp poprzez przeglądarkę Web, SSH;</li> <li>○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;</li> <li>○ Zarządzanie alarmami (zdarzenia poprzez SNMP)</li> <li>○ Możliwość przejścia konsoli tekstowej</li> <li>○ Możliwość zarządzania przez 6 administratorów jednocześnie</li> <li>○ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) - funkcjonalność aktywna dożywotnio, bez żadnych ograniczeń;</li> <li>○ Obsługa serwerów proxy (autentykacja)</li> <li>○ Obsługa VLAN</li> <li>○ Możliwość konfiguracji parametru Max. Transmission Unit (MTU)</li> <li>○ Wsparcie dla protokołu SSDP</li> <li>○ Obsługa protokołów TLS 1.2, SSL v3</li> <li>○ Obsługa protokołu LDAP</li> <li>○ Integracja z HP SIM</li> <li>○ Synchronizacja czasu poprzez protokół NTP</li> <li>○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej</li> </ul> <p>Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);</p> <p>Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;</p>



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.</p>
Wspierane OS	<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2019, 2016</li> <li>• VMWare vSphere 6.7</li> <li>• Suse Linux Enterprise Server 12</li> <li>• Red Hat Enterprise Linux 7</li> </ul>
Gwarancja	<p>60 miesięcy gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem do miejsca użytkowania sprzętu certyfikowanego przez producenta pracownika serwisu do końca następnego dnia roboczego;</p> <p>Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu (bez udziału administratora);</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;</p> <p>Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;</p> <p>Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);</p>
Dokumentacja, inne	<p>Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy;</p> <p>Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy;</p> <p>Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;</p> <p>W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;</p> <p>Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</p>



**Fundusze Europejskie**  
Polska Cyfrowa



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>Celem prac jest przygotowanie środowiska teleinformatycznego na potrzeby pracy w środowisku domenowym Active Directory urządzeń zainstalowanych w Urzędzie Gminy w Majdan Królewski.</p> <p>Część serwerowa powinna zostać oparta na systemie wirtualizacji zasobów IT</p>
--	---



**Fundusze Europejskie**  
Polska Cyfrowa



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

## Licencja Windows Server

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Oprogramowanie	<p>1) Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się, aby oferowane licencje umożliwiały korzystanie 55 użytkownikom.</p> <p>Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.</p> <p>2) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</p> <p>3) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</p> <p>4) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.</p> <p>5) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</p> <p>6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</p> <p>7) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</p> <p>8) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</p> <p>9) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</p> <p>10) Wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <p>a) pozwalają na zmianę rozmiaru w czasie pracy systemu,</p>





*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<ul style="list-style-type: none"> <li>b) umożliwiając tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>c) umożliwiając kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>d) umożliwiając zdefiniowanie list kontroli dostępu (ACL).</li> </ul> <ul style="list-style-type: none"> <li>11) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>12) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li> <li>13) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET</li> <li>14) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>15) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>16) Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ul style="list-style-type: none"> <li>a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b) Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych.</li> </ul> </li> <li>17) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</li> <li>18) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</li> <li>19) Mechanizmy logowania w oparciu o: <ul style="list-style-type: none"> <li>a) Login i hasło,</li> <li>b) Karty z certyfikatami (smartcard),</li> <li>c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> </ul> </li> <li>20) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..</li> <li>21) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>22) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> </ul>
--	---



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

- 23) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 24) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- 25) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- 26) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
  - a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
  - b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    - i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
    - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    - iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
  - c) Zdalna dystrybucja oprogramowania na stacje robocze.
  - d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
  - e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    - i. Dystrybucję certyfikatów poprzez http
    - ii. Konsolidację CA dla wielu lasów domeny,
    - iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    - iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
  - f) Szyfrowanie plików i folderów.



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</p> <p>i) Serwis udostępniania stron WWW.</p> <p>j) Wsparcie dla protokołu IP w wersji 6 (IPv6),</p> <p>k) Wsparcie dla algorytmów Suite B (RFC 4869),</p> <p>l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</p> <p>m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ul style="list-style-type: none"> <li>i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</li> <li>ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.</li> <li>iii. Obsługi 4-KB sektorów dysków</li> <li>iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra</li> <li>v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.</li> <li>vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)</li> </ul> <p>27) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p>
--	---



Fundusze  
Europejskie  
Polska Cyfrowa



Rzeczpospolita  
Polska

Unia Europejska  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

	<p>28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>29) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>30) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>31) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>Zorganizowany system szkoleń i materiały edukacyjne w języku polskim</p>
--	---



**Fundusze Europejskie**  
Polska Cyfrowa



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

## Urządzenie NAS wraz z dyskami

Nazwa komponentu	Wymagane minimalne parametry techniczne
Liczba procesorów	Min 1
Architektura procesora	x86
Częstotliwość procesora	Min 4-core 2.2 GHz Procesor osiągający w teście PassMark CPU Mark wynik min. 4500 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: <a href="http://www.cpubenchmark.net">www.cpubenchmark.net</a> , nie wcześniej niż 20.07.2022r)
Pamięć systemowa	Min 4GB
Całkowita liczba gniazd pamięci	1
Maksymalna pojemność pamięci	Min 32 GB
Kieszeń/kieszenie na dyski	Min 6
Kieszenie dysków M.2 <sub>2</sub> (NVMe)	Min 2
Zainstalowane dyski zgodne z tabelą kompatybilności producenta urządzenia	Min 6x 6 TB Pamięć podręczna 256MB - Prędkość obrotowa 7200 obr./min - Niezawodność 1 000 000 godz
Zgodny typ dysków obsługiwanych	3.5" SATA HDD 2.5" SATA HDD 2.5" SATA SSD M.2 2280 NVMe SSD
Port LAN RJ-45 1GbE z obsługą	Min 4 szt



**Fundusze Europejskie**  
Polska Cyfrowa



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz  
Rozwoju Regionalnego



*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

funkcji Link Aggregation / przełączania awaryjnego	
Port USB 3.2 1. generacji	Min 3 szt
Gwarancja	Minimum 36 miesięcy