Załącznik nr 6 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowa Gmina" realizowanego przez Gminę Żagań o statusie miejskim.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina" dla Gminy Żagań o statusie miejskim.

Zamówienie zostało podzielone na części:

- CZEŚĆ I - Dostawa sprzętu komputowego
- CZĘŚĆ II – Dostawa skanerów
- CZĘŚĆ III – Rozbudowa zabezpieczeń logicznych

Cześć I: Dostawa sprzętu komputowego

Serwer Typ I

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Z organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor min 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 231 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	minimum jeden sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5" Hot-Plug skonfigurowane do intensywnego odczytu Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację

	poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/dodatkowe oprogramowanie	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo wraz z licencją dostępową dla 120 użytkowników. Licencja powinna pozwalać na użytkowanie minimum jednej poprzedniej wersji oprogramowania. Wraz z oprogramowaniem powinien zostać dołączony nośnik umożliwiający zainstalowanie poprzedniej wersji oprogramowania. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania. SSO musi posiadać następujące, wbudowane cechy: • możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, • możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, • możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, • 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, • wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, • wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, • automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, • możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), • wbudowane wsparcie instalacji i pracy na wolumenach, które: ○ pozwalają na zmianę rozmiaru w czasie pracy systemu,

	○ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, ○ umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, ○ umożliwiają zdefiniowanie list kontroli dostępu (ACL), • wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, • wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 • możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, • możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, • wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, • graficzny interfejs użytkownika, • zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, • wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), • możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, • dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, • możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: ○ podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, ○ 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: ■ podłączenie SSO do domeny w trybie offline –

	bez dostępnego połączenia sieciowego z domeną, ■ ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, ■ odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, ○ zdalna dystrybucja oprogramowania na stacje robocze, ○ praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, ○ centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ■ dystrybucję certyfikatów poprzez http, ■ konsolidację CA dla wielu lasów domeny, ■ automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ○ szyfrowanie plików i folderów, ○ szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), ○ możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, ○ serwis udostępniania stron WWW, ○ wsparcie dla protokołu IP w wersji 6 (IPv6), ○ wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: ■ dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	■ obsługi ramek typu jumbo frames dla maszyn wirtualnych, ■ obsługi 4-KB sektorów dysków, ■ nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, ■ możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, ■ możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), • możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, • wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 800W.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

	• Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty/normy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.

	Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu.
Warunki gwarancji	***Kryterium oceny ofert o wadze 40%:*** Zamawiający wymaga minimum 3 lat gwarancji. Wykonawca może zaoferować wiążący dla niego okres 5 lat gwarancji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta prowadzoną w języku polskim Zamawiający wymaga aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Możliwość sprawdzenia statusu gwarancji.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania wdrożeniowe	Zamawiający w ramach wdrożenia infrastruktury serwerowej wymaga: • aby Wykonawca stworzył plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie Serwera Wirtualizacyjnego w szafie rack zamawiającego. • montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. • Uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera. • podłączenia Serwera do Przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera • testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania

	• podłączenie dedykowanych portów zarządzających urządzeniami (wirtualna konsola KVM) do oddzielonej logicznie sieci (za pomocą vlanu/osobnej podsieci) – w przypadku konieczności konfiguracji osobnego vlanu/podsieci wymaga się aby wykonawca skonfigurował to w urządzeniu UTM/Router • instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie wraz • Konfigurację akcji "shutdown" w momencie zaniku zasilania na urządzeniu UPS • Uruchomienie usługi katalogowej oraz stworzenie dedykowanych użytkowników administracyjnych. Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.

Serwer Typ II

Nazwa	**Minimalne wymagania dla sprzętu**
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor minimum 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 231 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 3 dyski SSD SATA o pojemności min. 960GB[RA1] , 6Gb, 2,5" Hot-Plug. SSD do intensywnego odczytu. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/dodatkowe oprogramowanie	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja powinna pozwalać na użytkowanie minimum jednej poprzedniej wersji oprogramowania. Wraz z oprogramowaniem powinien zostać dołączony nośnik umożliwiający zainstalowanie poprzedniej wersji oprogramowania. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania. SSO musi posiadać następujące, wbudowane cechy: • możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, • możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, • możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, • 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, • wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,

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

	innych producentów wymagających dodatkowych licencji: ○ podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, ○ 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: ■ podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ■ ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, ■ odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, ○ zdalna dystrybucja oprogramowania na stacje robocze, ○ praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, ○ centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ■ dystrybucję certyfikatów poprzez http, ■ konsolidację CA dla wielu lasów domeny, ■ automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ○ szyfrowanie plików i folderów, ○ szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), ○ możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, ○ serwis udostępniania stron WWW, ○ wsparcie dla protokołu IP w wersji 6 (IPv6), ○ wbudowane mechanizmy wirtualizacji (Hypervisor)

	pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: ■ dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ■ obsługi ramek typu jumbo frames dla maszyn wirtualnych, ■ obsługi 4-KB sektorów dysków, ■ nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, ■ możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, ■ możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), • możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, • wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 800W.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory;

	• możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty/normy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną. Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu
Warunki gwarancji	***Kryterium oceny ofert o wadze 40%:*** Zamawiający wymaga minimum 3 lat gwarancji. Wykonawca może zaoferować wiążący dla niego okres 5 lat gwarancji, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta prowadzoną w języku polskim Zamawiający wymaga aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Możliwość sprawdzenia statusu gwarancji.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania wdrożeniowe	Zamawiający w ramach wdrożenia infrastruktury serwerowej wymaga: • aby Wykonawca stworzył plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie Serwera Wirtualizacyjnego w szafie rack zamawiającego. • montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych

	serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. • Uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera. • podłączenia Serwera do Przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera • testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania • podłączenie dedykowanych portów zarządzających urządzeniami (wirtualna konsola KVM) do oddzielonej logicznie sieci (za pomocą vlanu/osobnej podsieci) – w przypadku konieczności konfiguracji osobnego vlanu/podsieci wymaga się aby wykonawca skonfigurował to w urządzeniu UTM/Router • instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie • Konfigurację akcji "shutdown" w momencie zaniku zasilania na urządzeniu UPS Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.

Serwer Typ III

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor min 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowane do pracy z

	zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 231 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 3 dyski SSD SATA o pojemności min. 960GB , 12Gb, 2,5" Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/dodatkowe oprogramowanie	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja powinna pozwalać na użytkowanie minimum jednej poprzedniej wersji oprogramowania. Wraz z oprogramowaniem powinien zostać dołączony nośnik umożliwiający zainstalowanie poprzedniej wersji oprogramowania. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania. SSO musi posiadać następujące, wbudowane cechy:

	• możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
	• możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
	• możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,
	• 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,
	• wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
	• wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
	• automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,
	• możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
	• wbudowane wsparcie instalacji i pracy na wolumenach, które:
	  ○ pozwalają na zmianę rozmiaru w czasie pracy systemu,
	  ○ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	  ○ umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	  ○ umożliwiają zdefiniowanie list kontroli dostępu (ACL),
	• wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
	• wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2
	• możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
	• możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
	• wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,

	• graficzny interfejs użytkownika,
	• zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
	• wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
	• możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
	• dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
	• możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	  ○ podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	  ○ 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:
	  ■ podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	  ■ ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
	  ■ odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
	  ○ zdalna dystrybucja oprogramowania na stacje robocze,
	  ○ praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
	  ○ centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
	  ■ dystrybucję certyfikatów poprzez http,

	■ konsolidację CA dla wielu lasów domeny, ■ automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ○ szyfrowanie plików i folderów, ○ szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), ○ możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, ○ serwis udostępniania stron WWW, ○ wsparcie dla protokołu IP w wersji 6 (IPv6), ○ wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: ■ dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ■ obsługi ramek typu jumbo frames dla maszyn wirtualnych, ■ obsługi 4-KB sektorów dysków, ■ nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, ■ możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, ■ możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny

	wirtualnej (tzw. trunk model), • możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, • wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 800W.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty/normy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu.
Warunki gwarancji	***Kryterium oceny ofert o wadze 40%:*** Zamawiający wymaga minimum 3 lat gwarancji. Wykonawca może zaoferować wiążący dla niego okres 5 lat gwarancji z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną prowadzoną w języku polskim

	Zamawiający wymaga aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego Możliwość sprawdzenia statusu gwarancji .
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania wdrożeniowe	Zamawiający w ramach wdrożenia infrastruktury serwerowej wymaga: • aby Wykonawca stworzył plan wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie Serwera Wirtualizacyjnego w szafie rack zamawiającego. • montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. • Uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera. • podłączenia Serwera do Przełącznika za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera • testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania • podłączenie dedykowanych portów zarządzających urządzeniami (wirtualna konsola KVM) do oddzielonej logicznie sieci (za pomocą vlanu/osobnej podsieci) – w przypadku konieczności konfiguracji osobnego vlanu/podsieci wymaga się aby wykonawca skonfigurował to w urządzeniu UTM/Router • instalacji oprogramowania wirtualizacyjnego na dostarczonym sprzęcie • Konfigurację akcji "shutdown" w momencie zaniku zasilania na urządzeniu UPS • Wymaga się dodanie serwera do usługi katalogowej jako zapasowy kontroler domeny z opcjami odczytu/zapisu. Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.

Przełączniki sieciowe Typ I

Nazwa	Minimalne wymagania dla oprogramowania
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 48 porty 10/100/1000Mbps RJ45, minimum 2 porty SFP/SFP+ 1/10GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 8000 adresów MAC Switch fabric capacity min. 100Gbps Forwarding rate min. 100Mpps Pamięć flash min. 128MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Możliwość połączenia w stos do 4 urządzeń tego samego typu Wydajność połączenia pomiędzy przełącznikami w stosie min. 20Gbps Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIv2 2246 TLS v1 2271 SNMP Framework MIB

	2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9) 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
ilość	1 szt.

Przełączniki sieciowe Typ II

Nazwa	**Minimalne wymagania dla oprogramowania**
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 16 portów 10/100/1000Mbps RJ45, minimum 2 porty SFP 1GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX
Wydajność przełącznika	Minimum 8000 adresów MAC Switch fabric capacity min. 80Gbps Forwarding rate min. 80Mpps Pamięć flash min. 128MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP

	802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIv2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIv2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9) 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Inne	Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza
ilość	2 szt.

UPS

Nazwa	**Minimalne wymagania dla sprzętu**	
Typ	Zasilacz awaryjny UPS	
Wymagania techniczne	Moc pozorna	min. 3000VA
	Moc rzeczywista	min. 3000W

	Technologia	on-line (VFI), podwójna konwersja
	Sprawność max (dla VFI)	> 90 %
	Typ obudowy	rack; z możliwością instalacji jako tower
	Ilość wydzielanego ciepła dla nominalnych warunków pracy	< 1200 BTU / h
	Praca sieciowa w zakresie minimum:	
	Napięcie wejściowe	110 ÷ 300 V AC ± 5%
	Częstotliwość napięcia wejściowego	50 / 60 Hz
	Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC ± 1 %
	Wartość napięcia wyjściowego ustawiana z panelu LCD	tak
	Kształt napięcia wyjściowego	sinusoidalny
	Czas przełączania sieć – UPS	0ms
	Współczynnik odkształceń prądu wejściowego THDi	< 10%
	Praca bateryjna w zakresie minimum:	
	Napięcie wyjściowe	~230V
	Częstotliwość napięcia wyjściowego	50Hz/60Hz ± 0,5Hz
	Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
	Zabezpieczenie przeciwzwarciowe gniazd wyjściowych	Bezpiecznik automatyczny 16 A
	Zabezpieczenie przeciążeniowe	elektroniczne
	Akumulatory wewnętrzne w UPS	minimum 12V 9Ah; szczelne, bezobsługowe
	Czas podtrzymania (100 % Pmax) - przy zastosowaniu baterii wew.	minimum 3,5 min
	Czas ładowania baterii wew w UPS /w modułach bateryjnych (nie zależnie od ilości podłączonych	do 3h

	modułów) - po 80% wyładowaniu baterii	
	UPS / Moduły Bateryjne wyposażone w niezależne ładowanie z sieci	wymagane
	Pozostałe cechy w zakresie minimum	
	Przeciążalność	110 % ÷ 120 % = 60s, >120 % = 100ms
	Wejście zasilania	1 x IEC 320 C20 (16 A)
	Ilość i typ gniazd wyjściowych	min 8x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16 A), z czego minimum 4 gniazda sterowalne
	Sygnalizacja	Wyświetlacz LCD
	Test baterii	wymagana możliwość uruchomienia testu baterii przyciskiem na obudowie zasilacza
	Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia do 10 zewnętrznych modułów bateryjnych
	Możliwość pracy w trybie konwertera częstotliwości	wymagane
	Interfejs komunikacyjny	RS232, USB HID, SNMP
	Przewody	min 1szt USB + 2szt IEC 320 C13-C14 10A + 1szt IEC 320 C19-C20 16A
	Wsporniki do montażu w szafie RACK	wymagane
	Remote ON/OFF – możliwość zdalnego załączenia/wyłączenia zasilacza	wymagane
	Złącze EPO	wymagane ustawienie NC
Gwarancja	minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory;	
Serwis	Serwis w języku polskim a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. Naprawa w maksymalnie 5 dni roboczych, Serwis realizowany w systemie door to door	

Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer. Oprogramowanie pozwala na możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPSów. Oprogramowanie pozwala na możliwość zarządzania różnymi UPSami tego samego producenta.
Certyfikaty producenta	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; deklaracja CE producenta sprzętu
Wymagania wdrożeniowe	• Wymaga się zainstalowania UPS w szafie rack Zamawiającego w sposób właściwy i zgodny z instrukcją montażową • Wymaga się aby skonfigurować adresację sieciową urządzenia UPS oraz zainstalować i skonfigurować oprogramowanie zamykające środowisko serwerowe na minimum 3 serwerach z systemem operacyjnym dostarczonym do serwerów z niniejszego postępowania.
Ilość	3 szt.

Mobilne stacje robocze

Nazwa	Minimalne wymagania dla sprzętu
Typ	Komputer przenośny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Matryca	Matryca o przekątnej 15.6” z powłoką przeciwodblaskową i rozdzielczością 1920 x 1080. Jasność matrycy min. 250 cd/m2, kontrast min. 700:1.
Procesor	Procesor osiągający w teście PassMark Performance Test, co najmniej 10,136 punktów w kategorii Average CPU Mark, według danych opublikowanych w dowolnym dniu pomiędzy dniem ogłoszenia o zamówieniu a terminem składania ofert. Wydruk ze strony należy dołączyć do oferty.
Pamięć RAM	8GB DDR4 3200MHz możliwość rozbudowy do min 32GB,
Pamięć masowa	512GB SSD NVMe Możliwość zainstalowania dodatkowego dysku 2,5”
Karta graficzna	Zintegrowana z procesorem
Klawiatura	Klawiatura w układzie US - QWERTY z wydzieloną klawiaturą numeryczną oraz z wbudowanym w klawiaturze podświetleniem. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2 x 2W. Czytnik kart multimedialnych w formacie microSD, Złącze audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Karta Wireless AX 2x2 + Bluetooth 5.1
Bateria i zasilanie	Bateria Polymer min. 3-cell [min. 41Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.
Waga	Waga max 2kg z baterią 3-cell Suma wymiarów notebooka nie większa niż 622mm (mierzone po krawędziach)
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, uszczelnienie dookoła matrycy chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni.
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz

	samego urządzenia wskazującego (wmontowanego na stałe). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i maks osiąganej prędkości, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag, nie podlegające skasowaniu nawet po aktualizacji BIOS. Funkcja logowania się do BIOS na podstawie hasła użytkownika i administratora (hasła niezależne), możliwość ustawienia haseł administratora oraz użytkownika składających się z małych liter, dużych liter, cyfr, znaków specjalnych. BIOS zawierający informację o stanie naładowania baterii, mocy podpiętego zasilacza, ponadto możliwość zarządzania trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
Certyfikaty	Certyfikat ISO9001 lub inny równoważny dla producenta sprzętu. Certyfikat ISO 14001 lub inny równoważny dla producenta sprzętu. Deklaracja zgodności CE.
System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych: lupa powiększająca zawartość ekranu, ● narrator odczytujący zawartość ekranu, ● regulacja jasności i kontrastu ekranu, ● możliwość odwrócenia kolorów np. biały tekst na czarnym tle, ● poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, ● funkcja sterowania myszą z klawiatury numerycznej, ● funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, ● korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, ● funkcja napisów w treściach wideo, ● możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 16. Możliwość zarządzania stacją roboczą poprzez polityki. 17. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 18. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 19. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 20. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 21. Graficzne środowisko instalacji i konfiguracji.

	22. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 23. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 24. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania plików systemowych. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych i dodatkowych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.
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.
Porty i złącza	Wbudowane porty i złącza: 1 x HDMI 1.4, 1x RJ-45, 1 x USB 2.0, 2 x USB 3.2 typu A, w tym jeden dosilony, 1x USB 3.2 gen 2 typu C, port zasilania, , gniazdo linki zabezpieczającej.
Oprogramowanie dodatkowe	Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji : a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Oprogramowanie biurowe	Zamawiający wymaga aby dostarczone notebooki posiadały preinstalowane oprogramowanie biurowe.

	Zamawiający oczekuje dostarczenia pakietu biurowego w modelu licencjonowania odpowiedniego dla pracowników urzędu, spełniającym następujące warunki: • licencja komercyjna, nieograniczona czasowo, bez konieczności wnoszenia dodatkowych opłat, • możliwość pobierania oprogramowania do instalacji ze strony producenta oprogramowania po uprzednim zalogowaniu, • pracujący pod kontrolą systemu operacyjnego min. z rodziny Windows tj.: Microsoft Windows 8, 10, 11 • oprogramowanie biurowe - ma zaimplementowane co najmniej następujące funkcjonalności tj. edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO) w domenie, • całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie, • wsparcie dla formatu XML, • możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów, • możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, • możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych, w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu, • prawidłowe odczytywanie i zapisywanie danych w dokumentach min. w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w tym plikach wytworzonych w MS Office 2007, MS Office 2010 i MS Office 2013, Office 2016 • zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). Musi być kompatybilny z posiadanym przez Zamawiającego oprogramowaniem Microsoft Office i pozwalać min. na: • otwieranie dokumentów utworzonych przy pomocy programów MS Word (od wersji 2007 do 2016), MS Excel (od wersji 2007 do 2016), MS Power Point (od wersji 2007 do 2016), • w otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (min.: korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze.) czy też konieczności dodatkowej edycji ze strony użytkownika. Edytor tekstów musi umożliwiać min.: • edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • sprawdzanie pisowni w języku polskim, • śledzenie zmian wprowadzonych przez użytkowników, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać min.: • 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 (min. inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), • tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • 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, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 do 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać min. przygotowywanie prezentacji multimedialnych oraz: • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie w postaci tylko do odczytu, • nagrywanie narracji dołączanej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • tworzenie animacji obiektów i całych slajdów. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać min.: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, • oznaczenie poczty elektronicznej z określeniem terminu przypomnienia, • zarządzanie kalendarzem, • zapraszanie uczestników na spotkanie, co po ich akceptacji musi spowodować automatyczne wprowadzenie spotkania w ich kalendarzach, • zarządzanie listą zadań, • zlecanie zadań innym użytkownikom, • zarządzanie listą kontaktów, • udostępnianie listy kontaktów innym użytkownikom, • przeglądanie listy kontaktów innych użytkowników, • możliwość przesyłania kontaktów innym użytkowników.
Wsparcie techniczne	Dedykowany portal techniczny, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)
Warunki gwarancyjne	3-letnia gwarancja świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data

	produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)
Ilość	21 sztuk

Stacje robocze z monitorem

Nazwa	Minimalne wymagania dla sprzętu
Typ	Komputer stacjonarny oraz monitor. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.
Wydajność obliczeniowa	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 12,425 punktów według danych opublikowanych w dowolnym dniu pomiędzy dniem ogłoszenia o zamówieniu a terminem składania ofert. Wydruk ze strony należy dołączyć do oferty.
Pamięć RAM	16GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB.
Pamięć masowa	Dysk M.2 SSD 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”
Karta graficzna	Zintegrowana z procesorem
Klawiatura	Klawiatura USB w układzie polski programisty
Mysz	Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
Wirtualizacja	Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 26 dB.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego.

	Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera (lub na jego zlecenie), zawierający nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Certyfikaty i standardy	Deklaracja zgodności CE lub inny równoważny Urządzenia muszą być wyprodukowane zgodnie z normą PN-EN ISO 50001 oraz ISO 9001
System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych: lupa powiększająca zawartość ekranu, ● narrator odczytujący zawartość ekranu, ● regulacja jasności i kontrastu ekranu, ● możliwość odwrócenia kolorów np. biały tekst na czarnym tle,

	● poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, ● funkcja sterowania myszą z klawiatury numerycznej, ● funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, ● korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, ● funkcja napisów w treściach wideo, ● możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 16. Możliwość zarządzania stacją roboczą poprzez polityki. 17. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 18. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 19. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 20. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 21. Graficzne środowisko instalacji i konfiguracji. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 23. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 24. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania plików systemowych. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). Klucz licencyjny systemu operacyjnego musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.
Wymagania dodatkowe	Wbudowane porty: 2x Display Port 1.4, port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w tym min 2 porty USB na przednim panelu obudowy i min. 4 porty USB 3.2 gen. 1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.

Oprogramowanie dodatkowe	Oprogramowanie zarządzające producenta komputera, instalowane na etapie produkcji komputera, umożliwiające min.: • monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów • powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu • powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów • śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. • Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: • upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, • możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, jakiego komponentu sprzętu dotyczy aktualizacja, wszystkich poprzednich aktualizacjach z informacjami jak powyżej. • wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne • możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. • rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) • sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) • dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml • raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Oprogramowanie biurowe	Zamawiający wymaga aby dostarczone komputery posiadały preinstalowane oprogramowanie biurowe. Zamawiający oczekuje dostarczenia pakietu biurowego w modelu licencjonowania odpowiedniego dla pracowników urzędu, spełniającym następujące warunki: • licencja komercyjna, nieograniczona czasowo, bez konieczności wnoszenia dodatkowych opłat, • możliwość pobierania oprogramowania do instalacji ze strony producenta oprogramowania po uprzednim zalogowaniu, • pracujący pod kontrolą systemu operacyjnego min. z rodziny Windows tj.: Microsoft Windows 8, 10, 11 • oprogramowanie biurowe - ma zaimplementowane co najmniej następujące funkcjonalności tj. edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej i kalendarza, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • możliwość zdalnej instalacji pakietu poprzez zasady grup (GPO) w domenie, • całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie, • wsparcie dla formatu XML,

	• możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów, • możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony, • możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych, w wypadku nieoczekiwanego zamknięcia aplikacji spowodowanego zanikiem prądu, • prawidłowe odczytywanie i zapisywanie danych w dokumentach min. w formatach: .DOC, .DOCX, XLS, .XLSX, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł, formularzy w tym plikach wytworzonych w MS Office 2007, MS Office 2010 i MS Office 2013, Office 2016 • zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). Musi być kompatybilny z posiadanym przez Zamawiającego oprogramowaniem Microsoft Office i pozwalać min. na: • otwieranie dokumentów utworzonych przy pomocy programów MS Word (od wersji 2007 do 2016), MS Excel (od wersji 2007 do 2016), MS Power Point (od wersji 2007 do 2016), • w otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (min.: korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze.) czy też konieczności dodatkowej edycji ze strony użytkownika. Edytor tekstów musi umożliwiać min.: • edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • sprawdzanie pisowni w języku polskim, • śledzenie zmian wprowadzonych przez użytkowników, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Arkusz kalkulacyjny musi umożliwiać min.: • 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 (min. inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), • tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • 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, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 do 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać min. przygotowywanie prezentacji multimedialnych oraz:

	• drukowanie w formacie umożliwiającym robienie notatek, • zapisanie w postaci tylko do odczytu, • nagrywanie narracji dołączanej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • tworzenie animacji obiektów i całych slajdów. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać min.: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, • oznaczenie poczty elektronicznej z określeniem terminu przypomnienia, • zarządzanie kalendarzem, • zapraszanie uczestników na spotkanie, co po ich akceptacji musi spowodować automatyczne wprowadzenie spotkania w ich kalendarzach, • zarządzanie listą zadań, • zlecanie zadań innym użytkownikom, • zarządzanie listą kontaktów, • udostępnianie listy kontaktów innym użytkownikom, • przeglądanie listy kontaktów innych użytkowników, • możliwość przesyłania kontaktów innym użytkowników.
Wsparcie techniczne	Dedykowany portal techniczny, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancyjne	3-letnia gwarancja świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Monitor	Monitor musi posiadać parametry w zakresie minimum: • Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8” (16:9) • Technologia wykonania matrycy: IPS • Rozmiar plamki: Maksymalnie 0,275mm • Jasność: min. 250 cd/m2 • Kontrast: Typowy 1000:1 • Kąty widzenia (pion/poziom): min. 178/178 stopni • Czas reakcji matrycy: max. 8 ms • Rozdzielczość maksymalna: 1920 x 1080 przy 60Hz • Paleta kolorów: 83% (CIE 1976) • Głębia kolorów: 16,7 miliona kolorów • Zyżycie energii: Maks. 30W (W trybie uśpienia maks. 0,3W) • Powłoka powierzchni ekranu: Antyodblaskowa • Podświetlenie: System podświetlenia LED

	• Bezpieczeństwo: Monitor musi być wyposażony w tzw. gniazdo zabezpieczenia przed kradzieżą. Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie. • Pochylenie monitora: min. 26 stopni • Złącza: min. 1x D-Sub, min. 1x Display Port 1.2 • Inne: Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm. • Gwarancja: 3 lata, możliwość zgłaszania awarii przez linię telefoniczną i stronę internetową. Czas reakcji serwisu - do końca następnego dnia roboczego. • Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego
Ilość	10 kompletów

Oprogramowanie do backupu

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	**Oprogramowanie do backupu stacji roboczych, serwerów oraz hostów wirtualnych**
Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk serwerowych.	
Wspierane systemy operacyjne	Oprogramowanie musi wspierać co najmniej systemy operacyjne: • Windows XP i nowsze. • Windows Server 2003 i nowsze. • Windows SBS 2011/2008, 2003/2003R2. • Windows Storage Server 2012/2012R2, 2008R2/2008/2003. • Windows MultiPoint Server 2012/2011/2010. • Linux.
Zarządzanie systemem kopii zapasowych	Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: • Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). • Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. • Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu). • Możliwość definiowania uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.). • Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami. • Wsparcie dla Single Sign On dla logowania do systemu. • Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. • Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). • Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. • Możliwość zdalnej instalacji agentów kopi zapasowych na maszynach z systemem operacyjnym Windows. • Możliwość zdalnego uaktualniania agentów kopi zapasowych. • Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.

	• Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej). • Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych. • Centralny katalog wszystkich danych zapisanych w kopiach zapasowych. • Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
Wykonywanie kopii zapasowych	Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: • Kopie zapasowe całych dysków i partycji. • Kopie zapasowe wybranych plików i folderów. • Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory) • Kopie zapasowe baz danych Oracle. • Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. • Zapis kopii zapasowych na udziały sieciowe. • Zapis kopii zapasowych na serwer SFTP. • Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). • Możliwość wyszukiwania plików w kopiach zapasowych. • Możliwość szyfrowania plików kopi zapasowych. • Wsparcia dla technologii VSS. • Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • Kompresja plików kopi zapasowych. • Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy). • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
Mechanizm odtwarzania kopii zapasowych	Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej: • Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore. • Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. • Odtworzenie poszczególnych plików i folderów. • Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania). • Granularne odtwarzanie baz danych Microsoft Exchange. • Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange. • Wyszukiwanie i podgląd odtwarzanych wiadomości email. • Granularne odtwarzanie baz danych Microsoft SQL. • Możliwość granularnego odtwarzania witryn i plików Microsoft SharePoint. • Odtwarzanie kontrolerów domeny Microsoft Active Directory. • Granularne odtwarzanie baz danych Oracle.
Dodatkowe wymagania	Dodatkowe wymagania związane ochroną danych: Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
Warunki licencjonowania	Licencja 3 letnia, pozwalająca na backup 3 serwerów.
Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk wirtualizacyjnych	

Wspierane systemy operacyjne	Oprogramowanie musi wspierać co najmniej systemy operacyjne:
	• Dla hosta:
	  ○ VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6,7.
	  ○ Hyper-V.
	  ○ Citrix XenServer.
	  ○ Red Hat Virtualization.

	○ Linux KVM. ○ Oracle VM Server. ● Dla maszyn wirtualnych: ○ Windows XP (SP3) i nowsze. ○ Windows Server 2003 i nowsze. ○ Windows SBS 2011/2008, 2003/2003R2. ○ Windows Storage Server 2012/2012R2, 2008R2/2008/2003. ○ Windows MultiPoint Server 2012/2011/2010. ○ Linux OS. ○ macOS.
Zarządzanie systemem kopii zapasowych	Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: ● Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. ● Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). ● Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. ● Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu). ● Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.). ● Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami. ● Wsparcie dla Single Sign On dla logowania do systemu. ● Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. ● Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). ● Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. ● Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows. ● Zdalne uaktualniania agentów kopi zapasowych. ● Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych. ● Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej). ● Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych. ● Centralny katalog wszystkich danych zapisanych w kopiach zapasowych ● Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
Wykonywanie kopii zapasowych	Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: ● Kopie zapasowe całych dysków i partycji. ● Kopie zapasowe wybranych plików i folderów. ● Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi). ● Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory) ● Kopie zapasowe baz danych Oracle. ● Kopie zapasowe hostów Hyper-V i VMWare ESXi. ● Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. ● Zapis kopi zapasowych na udziały sieciowe. ● Zapis kopi zapasowych na serwer SFTP..

	• Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). • Możliwość wyszukiwania plików w kopiach zapasowych. • Szyfrowanie plików kopi zapasowych. • Wsparcie dla technologii VSS. • Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • Kompresja plików kopi zapasowych. • Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy). • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
Mechanizm odtwarzania kopii zapasowych	Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej: • Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore • Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. • Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej. • Odtworzenie poszczególnych plików i folderów. • Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania). • Granularne odtwarzanie baz danych Microsoft Exchange. • Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange. • Wyszukiwanie i podgląd odtwarzanych wiadomości email. • Granularne odtwarzanie baz danych Microsoft SQL. • Granularne odtwarzanie witryn i plików Microsoft SharePoint. • Odtwarzanie kontrolerów domeny Microsoft Active Directory. • Granularne odtwarzanie baz danych Oracle. • Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
Dodatkowe wymagania	Dodatkowe wymagania związane ochroną danych: Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
Warunki licencjonowania	Licencja 3 letnia, pozwalająca na backup 2 hostów wirtualnych.
Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk stacji roboczych.	
Wspierane systemy operacyjne	Oprogramowanie musi wspierać fizyczne i wirtualne posiadane przez Zamawiajacego komputery z systemem operacyjnym Windows XP i nowsze oraz systemy macOS.
Zarządzanie systemem kopii zapasowych	Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: • Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). • Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. • Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu). • Możliwość definiowania uprawnień dla administratorów systemu kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).

	• Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami. • Wsparcie dla Single Sign On dla logowania do systemu. • Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. • Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). • Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. • Możliwość zdalnej instalacji agentów kopi zapasowych na maszynach z systemem operacyjnym Windows. • Możliwość zdalnego uaktualniania agentów kopi zapasowych. • Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych. • Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej). • Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych. • Centralny katalog wszystkich danych zapisanych w kopiach zapasowych. • Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
Wykonywanie kopii zapasowych	Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: • Kopie zapasowe całych dysków i partycji. • Kopie zapasowe wybranych plików i folderów. • Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. • Zapis kopi zapasowych na udziały sieciowe. • Zapis kopi zapasowych na serwer SFTP. • Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). • Możliwość wyszukiwania plików w kopiach zapasowych. • Możliwość szyfrowania plików kopi zapasowych. • Wsparcia dla technologii VSS. • Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • Kompresja plików kopi zapasowych. • Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, magazyn chmurowy). • Możliwość replikacji kopi zapasowych na nośniki taśmowe. • Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
Mechanizm odtwarzania kopii zapasowych	Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej: • Odtworzenie całej maszyny (Windows, Mac) – tzw. Bare Metal Restore. • Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. • Odtworzenie poszczególnych plików i folderów. • Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
Dodatkowe wymagania	Dodatkowe wymagania związane ochroną danych: Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
Warunki licencjonowania	Licencja 3 letnia, pozwalająca na backup 10 stacji roboczych.

Oprogramowanie do monitorowania sieci

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do monitorowania sieci.
Wymagania minimalne	Oprogramowanie powinno posiadać budowę modułową, powinno składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinno być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Oprogramowanie powinno umożliwiać jednoczesną pracę minimum dwóch Administratorów w tym samym czasie. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source, dzięki czemu nie powinien być objęty limitem ilości danych, baza danych powinna być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Główny Administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. powinien móc wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Oprogramowanie powinno posiadać funkcjonalności: 1. Monitorowanie infrastruktury w zakresie minimum: ● Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). ● Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci. ● Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. ● Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. ● Serwerów pocztowych: ○ program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, ○ program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, ○ program powinien mieć możliwość wykonywania operacji testowych, ○ program powinien mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa. ● Monitorowanie serwerów WWW i adresów URL. ● Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. ● Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP) ● Obsługa komunikatów syslog i pułapek SNMP. ● Monitoring routerów i przełączników wg: ○ zmian stanu interfejsów sieciowych, ○ ruchu sieciowego, ○ podłączonych stacji roboczych, ○ ruchu generowanego przez podłączone stacje robocze. ● Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego: ○ obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. 2. Gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie minimum: ● Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart ● Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.

	• Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. • Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP • Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. • Możliwość odczytania numeru seryjnego (klucze licencyjne). • Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. • Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań. 3. Umożliwianie monitorowania aktywności użytkownikówi w zakresie minimum: • Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. • Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. • Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). • Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). • Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. • Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. • Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. • Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. 4. Umożliwienie ochrony danych przed wyciekiem w zakresie minimum: • Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. • Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. • Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. • Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. • Autoryzowanie urządzeń firmowych: pendrive'ów, dysków zewnętrznych - urządzenia nieautoryzowane. • Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. • Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. • Możliwość usuwania z listy znanych urządzeń tych nośników.

	Program powinien pozwalać na Integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Powinien pozwalać również na przydzielanie uprawnień również do kont użytkowników lokalnych. Program powinien mieć ochronę przed usunięciem. Powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
Warunki licencji	Licencja na użytkowanie oprogramowania musi być wieczysta. Musi dawać możliwość wsparcia oraz aktualizacji przez okres 1 roku.
Wymagania wdrożeniowe	Zamawiający w ramach wdrożenia rozwiązania wymaga: • Przygotowanie maszyny wirtualnej/systemu operacyjnego do instalacji aplikacji serwera. • Instalacja i konfiguracja serwera aplikacji w sposób umożliwiający komunikację z urządzeniami końcowymi w sieci lokalnej. • Przeprowadzenie aktywacji oprogramowania • Konfiguracja urządzenia brzegowego (Router/UTM) w celu umożliwienia komunikacji urządzeń końcowych z serwerem, spoza sieci zamawiającego. • Wygenerowanie aplikacji/agentów dla urządzeń końcowych oraz ich masowe wdrożenie na stacjach roboczych. • Konfiguracja modułów aplikacji, w celu zbierania oraz przechowywania tylko informacji niezbędnych z punktu widzenia zamawiającego. • Utworzenie kont administracyjnych oraz konfiguracja ich uprawnień według wymagań zamawiającego. • Skonfigurowanie alarmów w przypadku zdarzeń monitorowanych przez oprogramowanie, według wymagań zamawiającego • Skonfigurowanie modułu zdalnej pomocy, utworzenie odpowiednich kont użytkowników. • Przeprowadzenie pierwszego skanowania sieci • Integracja serwera aplikacji z lokalnym serwerem Active Directory (o ile taka usługa działa u zamawiającego) • Utworzenie dodatkowych folderów/typów zasobów ułatwiających inwentaryzację, według potrzeb zamawiającego • Konfiguracja funkcji ochrony danych. W szczególności polityk blokowania oraz audytowania dostępu do konkretnych plików/katalogów/urządzeń wymiennych.
Ilość	120 szt. licencji

Urządzenie do backupu

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie typu NAS
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków SATA3 o maksymalnej pojemności 20TB każdy, wraz z kompletem szyn umożliwiających montaż w szafie rack. Na urządzeniu znajdują się wskaźniki LED informujące min o HDD 1-8, Status, LAN, USB, Zasilanie
Procesor	Zainstalowany jeden procesor 4-rdzeniowy, min. 3.3GHz, klasy x86 klasy serwerowej.
Koprocesor arytmetyczny	tak
Pamięć RAM	zainstalowane min. 8 GB UDIMM DDR4 ECC, możliwość rozszerzenia pamięci RAM min. do 128GB
Pamięć Flash	min. 5GB
Gniazda PCI	min. 4 gniazda:

	min. 3 x PCIe Gen2 x4 min. 1 x PCIe Gen3 x8
Interfejsy sieciowe	min. 4 x Gigabit (10/100/1000) min. 2 x SFP+ 10GbE obsługa VLAN i Jumbo Frame
Dyski twarde	zamontowane 5 sztuk dysków klasy enterprise o pojemności min 4TB z MTBF na poziomie 2 milionów godzin, 5-letnią gwarancją, min. 256MB Cache, 7200 RPM
Porty USB	Urządzenie posiada min. 2 porty typu C USB 3.1 Gen2, oraz min. 4 porty typu A USB 3.1 Gen2
Wspierane Systemy Operacyjne	Apple Mac OS 10.7 or later Linux and UNIX Microsoft Windows 7, 8, and 10 Microsoft Windows Server 2003, 2008 R2, 2012, 2012 R2, 2016 i 2019
Odsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10 i 10+Spare, 50, 60. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk. Urządzenie posiada także możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
Wentylatory	Minimum 2 każdy po 6 cm.
Zasilanie	Redundantne (2x 300W). Urządzenie posiada możliwość obsługi sieciowych awaryjnych zasilaczy UPS.
Stacja monitoringu	Obsługa do 80 kamer IP (8 licencje domyślnie)
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Serwer TFTP, Server VPN, Obsługa kontenerów (LXC, Docker), Autotiering, Migawki wolumenów (min. 1024)
Wirtualizacja	możliwość uruchomienia maszyn wirtualnych bezpośrednio na macierzy bez konieczność posiadania zewnętrznych wirtualizatorów
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Język GUI	Polski

Gwarancja	Gwarancja 36 miesięcy na NAS Gwarancja 60 miesięcy na dyski
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont urzytkownika	min. 4096
Liczba grup	512
Liczba udziałów	512
Maksymalna ilość połączeń	700
Wymagania wdrożeniowe	Zamawiający wymaga przeprowadzenia wdrożenia w minimalnym zakresie • Wymaga się zainstalowania urządzenia NAS w szafie rack Zamawiającego w sposób właściwy i zgodny z instrukcją montażową • Wymaga się skonfigurowania wolumenów w sposób ustalony z Zamawiającym na etapie dostawy, właściwy RAID. • Konfigurację powiadomień SMTP/SNMP • Konfigurację protokołu LACP lub innego gwarantującego nadmiarowość połączeń LAN • Aktualizację urządzenia do najnowszego wersji systemu operacyjnego na dzień wdrożenia • Dodanie urządzenia do usługi katalogowej oraz konfiguracja uprawnień na poszczególnych wolumenach/katalogach udostępnionych (3 katalogi maks) • Konfiguracji funkcji migawkowych Wymaga się wdrożenia przez inżyniera z minimum 3 letnim doświadczeniem we wdrażaniu tego typu urządzeń NAS.
Ilość	3 szt.

Oprogramowanie do szyfrowania maili

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Oprogramowanie do szyfrowania wiadomości email z technologią end to end.
Wymagania minimalne	Oprogramowanie musi zapewnić funkcjonalność: • szyfrowanie algorytmem AES256 treści wiadomości, • szyfrowanie algorytmem AES256 załączników, • szyfrowanie algorytmem AES256 plików, • szyfrowanie algorytmem AES256 katalogów, • do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego. • do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe. • do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego.

	• do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego. • odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0 • szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki, • generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania, • opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność, • zabezpieczenia każdego emaila dedykowanym unikalnym hasłem, • posiadania wewnętrznej bazy haseł, która umożliwia: ○ export haseł do pliku, ○ import haseł z pliku ○ generowania ponownie haseł w bazie • posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich, • posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym, • zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami. Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.
Zgodność z systemami operacyjnymi i standardami	Oprogramowanie musi współpracować z klientem MS Outlook i Mozilla Thunderbird oraz Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11 (posiadane przez Zamawiającego).
Warunki licencji	Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy. Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.
Wsparcie techniczne	Oprogramowanie musi posiadać wsparcie techniczne i prawo do aktualizacji przez min. 2 lata. W szczególności: wsparcie telefoniczne, mailowe, wsparcie przy pomocy technologii zdalnych połączeń przez internet. Wsparcie techniczne świadczone jest w języku polskim w godzinach 8:00-16:00 w dni robocze bezpośrednio.
Ilość	120 szt. licencji

Szkolenie dla administratorów z zakresu dostarczonej infrastruktury

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenie dla administratorów z zakresu dostarczonej infrastruktury
Infrastruktura serwerowa	Przeprowadzenie szkolenia z zarządzania niskopoziomowego dostarczanych serwerów obejmującego w minimalnym zakresie: • tworzenie grup RAID • obsługę wirtualnej konsoli (podłączanie napędów ISO) • diagnozowanie ewentualnych problemów • generowanie logów Przeprowadzenie szkolenia z zakresu wirtualizacji swym zakresem obejmującym: • tworzenie nowych maszyn wirtualnych oraz ich parametryzację (zarządzanie wirtualnymi kartami sieciowymi, pamięcią ram) • przedstawienie oraz charakterystyka oprogramowania do zarządzania środowiskiem wirtualizatorów • konfiguracje wirtualnej infrastruktury sieciowej (wirtualnego przełącznika) • przedstawienie i zarządzanie uprawnieniami użytkowników • usługi migawkowe dla maszyn wirtualnych

	• tworzenie i eksportowanie logów i konfiguracji oprogramowania wirtualizacyjnego Szkolenie dotyczące dodawania nowych komputerów do usługi katalogowej. Wymaga się aby szkolenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.
UPS	Wymagane jest szkolenie z obsługi oprogramowania UPS
Oprogramowanie do monitorowania sieci	Zamawiający wymaga przeprowadzenia instruktażu w minimalnym zakresie: • Ogólne omówienie dostarczonego rozwiązania • Wymagania i instalacja systemu • Wstępna konfiguracja systemu i instalacja • Konfiguracja i praca w poszczególnych modułach • Rozwiązywanie najczęstszych problemów
NAS	Zamawiający wymaga przeprowadzenia szkolenia w zakresie minimum: ○ Generowania logów ○ Zarządzania volumenami ○ Możliwości replikacji migawek ○ Zarządzania migawkami ○ Aktualizacji urządzenia Wymaga się aby szkolenie zostało przeprowadzone przez inżyniera z minimum 3 letnim doświadczeniem we wdrażaniu tego typu urządzeń NAS.

Wymagania dodatkowe

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Zamawiającego.

CZĘŚĆ II – Dostawa skanerów

Skaner Typ I

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Urządzenie wielofunkcyjne A4 monochromatyczne
Parametry techniczne	Parametry techniczne w zakresie minimum: • Prędkość druku: 43 str/min • Czas wydruku pierwszej strony: 6,4 sek • Interfejsy: USB 2.0 Hi-Speed, 10BASE-T/100BASE-TX/1000Base-T/bezprzewodowa sieć LAN (IEEE 802.11 b/g/n) • Wyświetlacz: kolorowy ekran dotykowy LCD TFT WVGA o przekątnej 12,7 cm / 5 cali • Prędkość drukowania jednostronnie A4 min. 43str./min • Rozdzielczość drukowania: 600x600 dpi • Podajnik dokumentów: jednoprzebiegowy automatyczny dwustronny podajnik dokumentów • Pojemność podajnika dokumentów: 50 arkuszy (80g/m2) • Prędkość skanowania: skanowanie dwustronne (cz.-b.): 70; skanowanie dwustronne (kol.): 26 • Rozdzielczość skanowania: 600x600 dpi • Język opisu strony: PCL 6, oryginalny Adobe PostScript3 • Dupleks automatyczny • Czas druku pierwszej strony maksymalnie 6,4 sek. • Czas nagrzewania od włączenia urządzenia maksymalnie 14 sek. • Kaseta na papier: min. 1 kaseta o pojemności min. 550 ark. (80g/m2) • Taca wielofunkcyjna na min. 100 arkuszy (80 g/m2) obsługująca gramaturę 60 – 199 g/m2 i formaty A6-A4 oraz obsługująca koperty: COM10, DL, C5, Monarch

	• Możliwość rozbudowy o dodatkowe kasety papieru: min. 3 kasety każda na 500 ark. (80g/m2) • Pojemność tacy odbiorczej: 150 arkuszy o gramaturze 80 g/m2 - wydrukiem do dołu
Wymagania dodatkowe	Urządzenie dostarczone wraz z tonerem wyprodukowanych przez producenta urządzenia: toner na min. 20.000 str (zgodnie z normą ISO/IEC 19752). Urządzenie musi być fabrycznie nowe i wyprodukowane w 2022 roku.
Certyfikaty	Certyfikat ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania i produkcji. Certyfikat ISO 14001:2015 dla producenta sprzętu, Deklaracja zgodności CE, Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego
Gwarancja i serwis	***Kryterium oceny ofert o wadze 40%:*** Zamawiający wymaga minimum 30 miesięcy gwarancji. Wykonawca może zaoferować wiążący dla niego okres 36 miesięcy gwarancji. Serwis świadczony w miejscu instalacji sprzętu z czasem reakcji do końca następnego dnia roboczego.
Ilość	8 szt.

Skaner Typ II

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Urządzenie wielofunkcyjne A3 kolorowe
	Parametry techniczne w zakresie minimum: • Format A3 • Drukowanie w kolorze • Automatyczny jednoprzebiegowy podajnik dokumentów do skanowania dwustronnego (dwustronny na dwustronny (automatycznie)), • Wbudowany moduł OCR bez limitu stron i licencji pozwalający skanować do formatów Word, PowerPoint, przeszukiwalnego PDF • Urządzenie wolnostojące. • Prędkość druku: A4 40 str./min kolor i mono, A3 21 str./min kolor i mono, • Czas wydruku pierwszej strony mono i kolor 7 sek. • Ekran dotykowy 10" • podajnik: 2 kasety - każda na 550 arkuszy o gramaturze 80 g/m^2 • Skanowanie jednostronne: 135/135 (300 × 300 dpi, wysyłanie), 80/80 (600 × 600 dpi, kopiowanie) • Skanowanie dwustronne: 270/270 (300 × 300 dpi, wysyłanie), 160/90 (600 × 600 dpi, kopiowanie) • Interfejsy podłączeniowe: SIEĆ: 1000Base-T/100Base-TX/10Base-T, bezprzewodowa sieć LAN (IEEE 802.11 b/g/n) INNE: 1 port USB 2.0 (host), 1 port USB 3.0 (host), 1 port USB 2.0 (urządzenie) • Maksymalna rozdzielczość druku 1200x1200 dpi • Języki opisu strony: UFR II, PCL6, Adobe® PostScript®3™ • Drukowanie bezpośrednie, obsługiwane typy plików: PDF, EPS, TIFF, JPEG, XPS • Procesor: 1,8 GHz 2 rdzenie • Pamięć 5GB i standardowo dysk twardy 250 GB SSD,
Wymagania dodatkowe	Urządzenie musi być fabrycznie nowe i wyprodukowane w 2022 roku.

Dodatkowe oprogramowanie	Wraz z urządzeniem dostarczone musi być oprogramowanie oparte na chmurze (bez potrzeby instalacji lokalnego serwera)do centralnego śledzenia i raportowania kosztów, generowanych przez poszczególnych użytkowników, powstałych poprzez wykonanie określonych ilości kopii/wydruków/skanów. Możliwość centralnego definiowania identyfikatorów użytkowników (numerów kart lub kodów PIN). Możliwość przydzielania uprawnień do poszczególnych funkcji urządzeń, np. kolor czy skanowanie. Możliwość rozbudowy o kolejne urządzenia tej samej marki, bez konieczności zakupu dodatkowych licencji.
Certyfikaty	Certyfikat ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania i produkcji. Certyfikat ISO 14001:2015 dla producenta sprzętu, Deklaracja zgodności CE, dokument potwierdzający, że firma serwisująca posiada ISO 9001:2015 na świadczenie usług serwisowych oraz posiadanie autoryzacji producenta urządzeń
Gwarancja i serwis	Zamawiający wymaga minimum 30 miesięcy gwarancji. Wykonawca może zaoferować wiążący dla niego okres 36 miesięcy gwarancji. Serwis świadczony w miejscu instalacji sprzętu z czasem reakcji do końca następnego dnia roboczego.
Ilość	2 szt.

Skaner Typ III

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Urządzenie wielofunkcyjne A4 kolorowe
Parametry techniczne	Parametry techniczne w zakresie minimum: • Drukowanie w kolorze, skanowanie, kopiowanie • Automatyczny podajnik dokumentów Jednoprzebiegowy podajnik na min 100ark. 80g/m^2 • Wbudowany moduł OCR bez limitu stron i licencji pozwalający skanować do formatów Word, PowerPoint, przeszukiwalnego PDF • Prędkość druku: 25 str./min kolor i mono • Czas nagrzewania maks. 10 sek. • Tryb szybkiego uruchamiania maks. 4 sek. • Ekran dotykowy, kolorowy, min. 10-calowy • Sieć: 10/100/1000, USB 2.0 (host) x 1, USB 3.0 (host) x 1, wifi • Maksymalna rozdzielczość druku 1200x1200 dpi • Języki opisu strony: PCL6, Adobe® PostScript®3™ • Drukowanie bezpośrednie, obsługiwane typy plików: PDF, EPS, TIFF, JPEG, XPS • Procesor: dwurdzeniowy procesor o częstotliwości 1,75 GHz • Pamięć 3GB i dysk twardy 250 GB
Wymagania dodatkowe	Urządzenie musi być fabrycznie nowe i wyprodukowane w 2022 roku.
Dodatkowe oprogramowanie	Wraz z urządzeniem dostarczone musi być oprogramowanie oparte na chmurze (bez potrzeby instalacji lokalnego serwera)do centralnego śledzenia i raportowania kosztów, generowanych przez poszczególnych użytkowników, powstałych poprzez wykonanie określonych ilości kopii/wydruków/skanów. Możliwość centralnego definiowania identyfikatorów użytkowników (numerów kart lub kodów PIN). Możliwość przydzielania uprawnień do poszczególnych funkcji urządzeń, np. kolor czy skanowanie. Możliwość rozbudowy o kolejne urządzenia tej samej marki, bez konieczności zakupu dodatkowych licencji.
Certyfikaty	Certyfikat ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania i produkcji. Certyfikat ISO 14001:2015 dla producenta sprzętu, Deklaracja zgodności CE,

	Firma serwisująca musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług serwisowych a świadczone usługi serwisowe nie mogą wpływać na ważność uprawnień gwarancyjnych Zamawiającego
Gwarancja i serwis	Zamawiający wymaga minimum 30 miesięcy gwarancji. Wykonawca może zaoferować wiążący dla niego okres 36 miesięcy gwarancji. Serwis świadczony w miejscu instalacji sprzętu z czasem reakcji do końca następnego dnia roboczego.
Ilość	2 szt.

CZĘŚĆ III – Rozbudowa zabezpieczeń logicznych

Urządzenie klasy UTM

Nazwa	Minimalne wymagania dla urządzenia
Typ	Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami oraz wdrożeniem
Wymagania techniczne	Dostarczone urządzenie klasy UTM musi posiadać następujące minimalne funkcje: 1. ELEMENTY SYSTEMU BEZPIECZEŃSTWA w zakresie minimum • Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu • Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q. • W zakresie Firewall, obsługa nie mniej niż 1 500 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę. • System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania. • Możliwość rozszerzenia pamięci do 2 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia • Musi posiadać 2x USB 3.0 z przodu urządzenia • System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu. • System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości • Systemy wirtualne muszą obsługiwać QOS • System pełniący funkcję zapory musi posiadać nie mniej niż: 2x SFP+, 8x SFP, 8x GE interfejsów. 2. FUNKCJONALNOŚĆ w zakresie minimum • Kontrola dostępu — zapora sieciowa Stateful Inspection • Ochrona przed wirusami - komercyjny antywirus [AV] • Poufność danych - IPSec VPN i SSL VPN • Kontrola witryn sieci Web — filtr URL • Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3) • Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN

	• Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji • Reputacja IP • Cloud Sandbox. 3. WYDAJNOŚĆ w zakresie minimum • Analiza ruchu szyfrowanego protokołem SSL • Wydajność Firewall co najmniej 10 Gb/s • Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 3 Gb/s • Wydajność ochrony przed atakami (IPS) minimum 5Gb/s • Wydajność AV nie mniej niż 4Gb/s. 4. FUNKCJONALNOŚĆ VPN w zakresie minimum • Wydajność IPSec VPN, nie mniej niż 5 Gb/s • Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja • Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem. • Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności • Praca w topologiach Hub and Spoke i Mesh • Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec, • Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24 • Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24 • Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) • Obsługa PnPVPN (Plug and Play VPN) • Wraz z dostawą urządzenie powinno posiadać 100x SSL VPN. 5. ROUTING w zakresie minimum • Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS • Obsługa Policy Based Routing • Funkcjonalność Virtual Wire. 6. TRANSLACJA ADRESÓW NAT w zakresie minimum • Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego. • Obsługa NAT46, NAT64, DNS64 • Wsparcie dla STUN. 7. POLITYKA BEZPIECZEŃSTWA SYSTEMU w zakresie minimum • Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety). • Możliwość budowania min. 8000 polityk • Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego • Musi być w stanie skonfigurować agregowane polityki • Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P). 8. WYDZIELENIE STREF BEZPIECZEŃSTWA w zakresie minimum • Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN • Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów • Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników. 9. OCHRONA ANTYWIRUSOWA w zakresie minimum • Silnik antywirusowy musi by ć oparty na przepływie tzw. flow-based • Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB • Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV • Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji. 10. RÓWNOWAŻENIE OBCIĄŻENIA w zakresie minimum • Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania

	• Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin • Kontrola stanu serwera, monitorowanie sesji i ochrona sesji. 11. OCHRONA IPS w zakresie minimum • Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury. • Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos. • Funkcjonalność zapobiegania atakom SQL injection, XSS injection • Możliwość budowania własnych niestandardowych reguł IPS. 12. OBRONA PRZED ATAKIEM w zakresie minimum • Ochrona przed nieprawidłowym działaniem protokołu • Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp. • Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood • Biała listę docelowych adresów IP. 13. KONTROLA APLIKACJI w zakresie minimum • Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP. • Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka. 14. FILTR ADRESÓW URL w zakresie minimum • Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków. • Możliwość zdefiniowania własnej bazy kategorii www. • Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL. • Kategoria takie jak hazard, malware, spam, botnety • Obsługa Safe Search • Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne • Dostosowanie strony ostrzeżenia. 15. OCHRONA DANYCH w zakresie minimum • Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy • Identyfikacja protokołu pliku, w tym HTTP、FTP、SMTP, POP3、IMAP • Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS • Filtrowanie plików przesyłanych przez SMB 16. REPUTACJA IP w zakresie minimum • Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force • Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP 17. ZAPOBIEGANIE BOTNETOM w zakresie minimum • Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware • Wsparcie DNS sinkhole • Wsparcie wykrywania tunelowania DNS • Wyrywanie i blokowanie DGA 18. CLOUD SANDBOX • Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń • Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB • Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów • Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń. 19. UWIERZYTELNIANIE UŻYTKOWNIKA • System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:

	- Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu - Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP - Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych - Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA • Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory • Wsparcie usług terminalowych • Uwierzytelnianie użytkownika przez Web przed dostępem do internetu • Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny 20. RAPORTOWANIE I PRZEGLĄDANIE LOGÓW • Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie • W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż: - Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego - Generowanie co najmniej 10 rodzajów raportów 21. SYSTEM LOGOWANIA • Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej. 22. CERTYFIKATY rozwiązanie musi: • posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall • być pozycjonowanym w raporcie Gartnera przez ostatnie 7 lat 23. ZARZĄDZANIE • Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych. • Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola • W celu rozbudowy oraz integralności systemu bezpieczeństwa urządzenie musi pochodzić od tego samego producenta co SBDS, XDR, NIPS i umożliwiać zarzadzanie wszystkimi urządzeniami z chmury producenta • Urządzenie powinno monitorować i graficznie prezentować stan pracy urządzenia. Parametry takie jak obciążenie CPU oraz pamięć z podziałem na procesy, wykres zajętości dysku twardego w czasie , temperaturę urządzania w wybranym przez administratora interwale czasowym oraz status zasilania i chłodzenia aktywnego
Gwarancja	***Kryterium oceny ofert o wadze 40%:*** Zamawiający wymaga minimum 30 miesięcy gwarancji oraz licencje dla wszystkich funkcji bezpieczeństwa na ten sam okres. Wykonawca może zaoferować wiążący dla niego okres 36 gwarancji na dostarczone elementy systemu oraz licencje, usługę NBD – Next Businees Day na 36 miesięcy.
Wymagania wdrożeniowe	Zamawiający w ramach wdrożenia wymaga wykonania następujących czynności: • Instalacja w szafie rack • Podpięcie weryfikacja statusu licencji, • Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, vlanów, połączeń PPPoE, konfiguracja grup agregacyjnych, konfiguracja routingu (dynamicznego, statycznego), SD-WAN, DHCP, DNS, NTP, konfiguracja raportów, zewnętrznych serwerów syslog, SNMP, wewnętrznego centrum certyfikacji np. na potrzeby VPN, QoS), • Konfiguracja serwera SMTP do powiadomień e-mailowych • Konfiguracja profilów administracyjnych wraz z określeniem polityk dostępu do administracji urządzeniem,

	• Konfiguracja mechanizmu automatycznych kopii zapasowych konfiguracji urządzenia,
	• Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy),
	• Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa,
	• Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa,
	• Konfiguracja lokalnej bazy użytkowników wraz z użytkownikami i grupami (na podstawie wcześniej przygotowanej listy) wraz z odpowiednimi dostępami oraz politykami FW oraz podłączenie do usługi LDAP/Active Directory wraz z konfiguracją dostępów oraz polityk FW,
	• Konfiguracja VPN wg potrzeby:
	  ○ Konfiguracja IPSec VPN site-to-site,
	  ○ Konfiguracja IPSec VPN client-to-site,
	  ○ Konfiguracja SSL VPN client-to-site,
	• Konfiguracja profilów kontroli Antywirusowej i podpięcie do polityk FW,
	• Konfiguracja profilów ochrony przed atakami IPS i podpięcie do polityk FW,
	• Konfiguracja profilów kontroli aplikacji i podpięcie do polityk FW,
	• Konfiguracja profilów kontroli WWW i podpięcie do polityk FW,
	• Konfiguracja profilów antyspamowych i podpięcie do polityk FW,
	• Test zastosowanych funkcji ochronnych,
	• Dostosowanie profilów IPS, Antywirus, Antyspam, filtrowania WWW do specyfiki sieci zamawiającego,
	• Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji.
	
	Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczonego rozwiązania klasy UTM danego producenta.

Ilość	1 szt.