Załącznik nr 1a do SIWZ

OPZ na sprzęt dla projektu EpiBaza

Spis treści

[1. Infrastruktura informatyczna 5](#_Toc2854128)

[1.1 Serwer typ 1 – 1 sztuka 5](#_Toc2854129)

[1.2 Serwer typ 2 – 3 sztuki 8](#_Toc2854130)

[1.3 Przełączniki sieciowe typ 1 – 3 sztuki 13](#_Toc2854131)

[1.4 Przełączniki sieciowe typ 2 – 2 sztuki 16](#_Toc2854132)

[1.5 Macierz dyskowa typ 1 – 1 sztuka 18](#_Toc2854133)

[1.6 Macierz dyskowa typ 2 – 1 sztuka 19](#_Toc2854134)

[1.7 Urządzenia zabezpieczające 20](#_Toc2854135)

[1.7.1 Sprzęt zabezpieczający klasy UTM (Unified Threat Management) – 1 sztuka 20](#_Toc2854136)

[1.7.1.1 Wymagania Ogólne 20](#_Toc2854137)

[1.7.1.2 Redundancja, monitoring i wykrywanie awarii 20](#_Toc2854138)

[1.7.1.3 Interfejsy, Dysk, Zasilanie 20](#_Toc2854139)

[1.7.1.4 Parametry wydajnościowe 21](#_Toc2854140)

[1.7.1.5 Funkcje Systemu Bezpieczeństwa 21](#_Toc2854141)

[1.7.1.6 Polityka Firewall 21](#_Toc2854142)

[1.7.1.7 Połączenia VPN 22](#_Toc2854143)

[1.7.1.8 Routing i obsługa łączy WAN 22](#_Toc2854144)

[1.7.1.9 Zarządzanie pasmem 22](#_Toc2854145)

[1.7.1.10 Kontrola Antywirusowa 23](#_Toc2854146)

[1.7.1.11 Ochrona przed atakami 23](#_Toc2854147)

[1.7.1.12 Kontrola aplikacji 23](#_Toc2854148)

[1.7.1.13 Kontrola WWW 23](#_Toc2854149)

[1.7.1.14 Uwierzytelnianie użytkowników w ramach sesji 24](#_Toc2854150)

[1.7.1.15 Zarządzanie 24](#_Toc2854151)

[1.7.1.16 Logowanie 24](#_Toc2854152)

[1.7.1.17 Certyfikaty 25](#_Toc2854153)

[1.7.1.18 Serwisy i licencje 25](#_Toc2854154)

[1.7.1.19 Gwarancja oraz wsparcie 25](#_Toc2854155)

[1.7.1.20 Uwagi dodatkowe 25](#_Toc2854156)

[1.7.2 Sprzęt zabezpieczający klasy WAF (Web Application Firewall) – 1 sztuka 26](#_Toc2854157)

[1.7.2.1 Wymagania Ogólne 26](#_Toc2854158)

[1.7.2.2 Architektura systemu 26](#_Toc2854159)

[1.7.2.3 Parametry fizyczne systemu 26](#_Toc2854160)

[1.7.2.4 Parametry wydajnościowe 27](#_Toc2854161)

[1.7.2.5 Podstawowe funkcje systemu 27](#_Toc2854162)

[1.7.2.6 Wymagane funkcje dodatkowe 28](#_Toc2854163)

[1.7.2.7 Zarządzanie 29](#_Toc2854164)

[1.7.2.8 Logowanie i Raportowanie 29](#_Toc2854165)

[1.7.2.9 Certyfikaty 29](#_Toc2854166)

[1.7.2.10 Sygnatury, subskrypcje 29](#_Toc2854167)

[1.7.2.11 Gwarancja oraz wsparcie 30](#_Toc2854168)

[1.7.2.12 Rozszerzone wsparcie serwisowe i uwagi dodatkowe 30](#_Toc2854169)

[1.7.3 Centralny system logowania 30](#_Toc2854170)

[1.7.3.1 Wymagania Ogólne 30](#_Toc2854171)

[1.7.3.2 Interfejsy, Dysk, Zasilanie 31](#_Toc2854173)

[1.7.3.3 Parametry wydajnościowe 31](#_Toc2854174)

[1.7.3.4 Gwarancja oraz wsparcie 32](#_Toc2854175)

[1.7.3.5 Rozszerzone wsparcie serwisowe i uwagi dodatkowe 33](#_Toc2854176)

[1.8 Komputer typu laptop 33](#_Toc2854177)

[1.8.1 Typ 1 – 2 sztuki 33](#_Toc2854178)

[1.8.2 Typ 2 – 7 sztuk 38](#_Toc2854179)

[1.9 Komputer typu stacjonarnego – 12 sztuk 42](#_Toc2854180)

[1.10 Monitor 24” – 12 szt. 48](#_Toc2854181)

[1.11 Urządzenie UPS dla komputerów stacjonarnych– 12 sztuk 49](#_Toc2854182)

[1.12 Urządzenia UPS dla serwerów – 2 sztuki 49](#_Toc2854183)

[1.13 Urządzenie wielofunkcyjne – 2 szt. 50](#_Toc2854184)

[2. Oprogramowanie 51](#_Toc2854185)

[2.1 Oprogramowanie do wirtualizacji 51](#_Toc2854186)

[2.1.1 Oprogramowanie do wirtualizacji dla serwerów wskazanych w pkt 1.1 51](#_Toc2854187)

[2.1.2 Oprogramowanie do wirtualizacji dla serwerów wskazanych w pkt 1.2 52](#_Toc2854188)

[2.1 Oprogramowanie do obsługi kopii zapasowych (backupowania) 53](#_Toc2854189)

[3. Wdrożenie i Usługi 58](#_Toc2854190)

# Infrastruktura informatyczna

## Serwer typ 1 – 1 sztuka

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej przeznaczonej dla systemów urządzeń mobilnych wykorzystywanych przez Zamawiającego (Adroid) oraz Apple iOS) przy użyciu jednego z protokołów NFC/BLE/WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być przeznaczona dla zainstalowanych procesorów, kompatybilna z nimi i zapewniająca bezawaryjną współpracę. |
| **Chipset** | Dedykowany do pracy w serwerach dwuprocesorowych i kompatybilny z zastosowanymi procesorami. |
| **Procesor** | Zainstalowany minimum jeden procesor klasy x86 co najmniej 4 rdzeniowy dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 541 w teście SPECint\_rate\_base2006, dostępnym na stronie www.spec.org dla dwóch procesorów. |
| **RAM** | Minimum 128GB DDR4 RDIMM min. 2666MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać minimum 3TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling  |
| **Gniazda PCI** | - minimum dwa sloty PCIe x16 generacji 3, obsługującej karty niskiego profilu „LowProfile” |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseTMożliwość instalacji wymiennie modułów udostępniających: - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT; - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+- cztery interfejsy sieciowe 1Gb Ethernet w standardzie SFP+;- dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.Dodatkowe dwie karty jednoportowe FC min. 8Gb/s. wraz z wkładką każda karta.  |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD, NVMe.Zainstalowane 2 dyski SSD SATA o pojemności min. 240GB, 6Gb/s, 2,5“ Hot-Plug skonfigurowane w RAID 1.Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 16GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy SAS 12Gbps obsługujący RAID 0, 1, 5, 10, 50. |
| **Napęd optyczny** | Niewymagany |
| **Wbudowane porty** | 4 x USB z czego nie mniej niż 1 na przednim panelu obudowy i jeden wewnętrzny, 2 x RJ-45, 2xVGA z czego jeden na panelu przednim, 1xRS-232. |
| **Video** | karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. Zamawiający dopuszcza karty zintegrowane. |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug min. 750W każdy. |
| **Bezpieczeństwo** | Wbudowany moduł TPM 2.0Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **Diagnostyka** | 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 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
* karta powinna mieć możliwość wyposażenia w wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.

Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:* wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
* możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
* wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
* możliwość oskryptowywania procesu wykrywania urządzeń;
* możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
* szczegółowy opis wykrytych systemów oraz ich komponentów;
* możliwość eksportu raportu do CSV, HTML, XLS;
* grupowanie urządzeń w oparciu o kryteria użytkownika;
* automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
* szybki podgląd stanu środowiska;
* podsumowanie stanu dla każdego urządzenia;
* szczegółowy status urządzenia/elementu/komponentu;
* generowanie alertów przy zmianie stanu urządzenia;
* filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
* integracja z service desk producenta dostarczonej platformy sprzętowej;
* możliwość przejęcia zdalnego pulpitu;
* możliwość podmontowania wirtualnego napędu;
* kreator umożliwiający dostosowanie akcji dla wybranych alertów;
* możliwość importu plików MIB;
* przesyłanie alertów „as-is” do innych konsol firm trzecich;
* aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
* możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
* możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
* moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych
 |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub normami równoważnymi. Serwer musi posiadać deklarację CE. |
| **Warunki gwarancji** | Minimum trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta lub wykonawcy lub dedykowaną stronę www producenta lub wykonawcy. W przypadku awarii nośników pozostają one własnością Zamawiającego.Zamawiający przewiduje opcję w postaci możliwości wydłużenia terminu gwarancji wykonawcy lub producenta do pięciu lat na poniższych warunkach:* Przedłużenie gwarancji nastąpi na warunkach takich samych lub korzystniejszych dla Zamawiającego jak dla okresu podstawowego;
* Przedłużenie nastąpi o okres 2 lat względem okresu podstawowego (trzyletniego), co w konsekwencji spowoduje, iż pełen okres gwarancji wyniesie 5 lat od dnia odbioru przedmiotu zamówienia;
* Przedłużenie nastąpi automatycznie po jednostronnym oświadczeniu Zamawiającego skierowanym do Wykonawcy. Zamawiający ma obowiązek złożyć takie oświadczenie przed upływem podstawowego terminu gwarancji;
* Wykonawcy nie przysługuje roszczenie o wydłużenie okresu gwarancji;
* Wykonawcy przysługiwać będzie wynagrodzenie za dodatkowy okres gwarancji zgodne z treścią oferty i umowy;
* Pozostałe warunki dotyczące realizacji zamówienia w zakresie opcji, zostały opisane we wzorze Umowy i SIWZ.
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego oraz poprzez stronę internetową sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego. |

## Serwer typ 2 – 3 sztuki

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej przeznaczonej dla systemów urządzeń mobilnych wykorzystywanych przez Zamawiającego (Adroid) oraz Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być przeznaczona dla zainstalowanych procesorów, kompatybilna z nimi i zapewniająca bezawaryjną współpracę. |
| **Chipset** | Dedykowany do pracy w serwerach dwuprocesorowych i kompatybilny z zastosowanymi procesorami. |
| **Procesor** | Zainstalowane dwa procesory min. 16-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 1510 w teście SPECint\_rate\_base2006, dostępnym na stronie www.spec.org dla dwóch procesorów. |
| **RAM** | Minimum 384GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać minimum 3TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling  |
| **Gniazda PCI** | - minimum dwa sloty PCIe x16 generacji 3, obsługującej karty niskiego profilu „LowProfile” |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseTMożliwość instalacji wymiennie modułów udostępniających: - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT; - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+- cztery interfejsy sieciowe 1Gb Ethernet w standardzie SFP+;- dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.Dodatkowe dwie karty jednoportowe FC min. 8Gb/s. wraz z wkładką każda karta.  |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD, NVMe.Zainstalowane 2 dyski SSD SATA o pojemności min. 240GB, 6Gb/s, 2,5“ Hot-Plug skonfigurowane w RAID 1.Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 16GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy SAS 12Gbps obsługujący RAID 0, 1, 5, 10, 50. |
| **Napęd optyczny** | Niewymagany |
| **Wbudowane porty** | 4 x USB z czego nie mniej niż 1 na przednim panelu obudowy i jeden wewnętrzny, 2 x RJ-45, 2xVGA z czego jeden na panelu przednim, 1xRS-232. |
| **Video** | karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. Zamawiający dopuszcza kartę zintegrowaną. |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug min. 750W każdy. |
| **Bezpieczeństwo** | Wbudowany moduł TPM 2.0Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **Diagnostyka** | Możliwość wyposażenia 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 posiadanym 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 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
* karta powinna mieć możliwość wyposażenia w wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.

Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:* wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
* możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
* wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
* możliwość oskryptowywania procesu wykrywania urządzeń;
* możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
* szczegółowy opis wykrytych systemów oraz ich komponentów;
* możliwość eksportu raportu do CSV, HTML, XLS;
* grupowanie urządzeń w oparciu o kryteria użytkownika;
* automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
* szybki podgląd stanu środowiska;
* podsumowanie stanu dla każdego urządzenia;
* szczegółowy status urządzenia/elementu/komponentu;
* generowanie alertów przy zmianie stanu urządzenia;
* filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
* integracja z service desk producenta dostarczonej platformy sprzętowej;
* możliwość przejęcia zdalnego pulpitu;
* możliwość podmontowania wirtualnego napędu;
* kreator umożliwiający dostosowanie akcji dla wybranych alertów;
* możliwość importu plików MIB;
* przesyłanie alertów „as-is” do innych konsol firm trzecich;
* aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
* możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
* możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
* moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych
 |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 14001 lub normami równoważnymi. Serwer musi posiadać deklarację CE. |
| **Warunki gwarancji** | Minimum trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta/wykonawcy lub dedykowaną stronę www producenta/wykonawcy. W przypadku awarii nośników pozostają one własnością Zamawiającego.Zamawiający przewiduje opcję w postaci możliwości wydłużenia terminu gwarancji wykonawcy lub producenta do pięciu lat na poniższych warunkach:* Przedłużenie gwarancji nastąpi na warunkach takich samych lub korzystniejszych dla Zamawiającego jak dla okresu podstawowego;
* Przedłużenie nastąpi o okres 2 lat względem okresu podstawowego (trzyletniego), co w konsekwencji spowoduje, iż pełen okres gwarancji wyniesie 5 lat od dnia odbioru przedmiotu zamówienia;
* Przedłużenie nastąpi automatycznie po jednostronnym oświadczeniu Zamawiającego skierowanym do Wykonawcy. Zamawiający ma obowiązek złożyć takie oświadczenie przed upływem podstawowego terminu gwarancji;
* Wykonawcy nie przysługuje roszczenie o wydłużenie okresu gwarancji;
* Wykonawcy przysługiwać będzie wynagrodzenie za dodatkowy okres gwarancji zgodne z treścią oferty i umowy;

Pozostałe warunki dotyczące realizacji zamówienia w zakresie opcji, zostały opisane we wzorze Umowy i SIWZ. |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego oraz poprzez stronę internetową sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego. |

## Przełączniki sieciowe typ 1 – 3 sztuki

|  |  |
| --- | --- |
|  | Minimalne wymagania |
| **Obudowa** | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz.Przełącznik bez wentylatorów (fanless) |
| **Porty** | Minimum 24 porty 10/100/1000Mbps RJ45, minimum 4 porty SFP/SFP+ 1/10GbE,1 port konsolowy mikro-USB. 1 port USB umożliwiający załadowanie konfiguracji dla przełącznika z pamięci flash USB |
| **Wydajność przełacznika** | Minimum 16000 adresów MACSwitch fabric capacity min. 128GbpsForwarding rate min. 96Mpps |
| Pamięć flash min. 1GBPamięć RAM min. 1GBBufor pamięci dla pakietów minimum 2MB |
| **Funkcjonalność warstwy II** |  |
| Obsługa minimum 512 wirtualnych sieciWsparcie dla agregacji LACP (802.3ad)Obsługa 64 grup LACP i 8 portów fizycznych per grupaObsługa technologii port mirroring oraz remote port mirroring |
| **Inne Funkcjonalności** |  |
| Możliwość połączenia w stos do 4 urządzeń tego samego typuWydajność połączenia pomiędzy przełącznikami w stosie min. 40GbpsObsługa 802.1x oraz Mac Based Authentication BypassObsługa list kontroli dostępu opartych o adresy MAC i IP Obługa minimum 100 list kontroli dostępu i 4000 reguł sumarycznie dla wszystkich listObsługa czasowych list kontroli dostępuObsługa min 8 kolejek QoS na port fizyczny Obsługa protokołu sflow |
| **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) RSTP-Per VLAN 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) |
|  |
| **Zgodnośc 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 1451 Manager-to- Manager MIB 1492 TACACS+ 1493 Managed Objects for Bridges MIB 1573 Evolution of Interfaces 1612 DNS Resolver MIB Extensions 1643 Ethernet-like MIB 1757 RMON MIB 1867 HTML/2.0 Forms with File Upload Extensions 1901 Community-based SNMPv2 1907 SNMPv2 MIB 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2068 HTTP/1.1 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIv2 2246 TLS v1 2271 SNMP Framework MIB 2295 Transport Content Negotiation 2296 Remote Variant Selection 2346 AES Ciphersuites for TLS 2576 Coexistence Between SNMPv1/v2/v3 2578 SMIv2 2579 Textual Conventions for SMIv2 2580 Conformance Statements for SMIv2 2613 RMON MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2665 Ethernet-like Interfaces MIB 2674 Extended Bridge MIB 2737 ENTITY MIB 2818 HTTP over TLS 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 3412 Message Processing and Dispatching 3413 SNMP Applications 3414 User-based security model 3415 View-based control model 3416 SNMPv2 3418 SNMP MIB 3577 RMON MIB 3580 802.1X with RADIUS 3737 Registry of RMOM MIB 4086 Randomness Requirements 4113 UDP MIB 4251 SSHv2 Protocol 4252 SSHv2 Authentication4253 SSHv2 Transport4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4521 LDAP Extensions 4716 SECSH Public Key File Format 6101 SSL |
| **Certyfikaty i standardy** | Zamawiający wymaga aby oferowany przełącznik: - został wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 14001 lub normami równoważnymi- posiadał deklarację CE- jest zgodny z standardem RoHS lub równoważnym |
| **Inne** | Przystosowanie do pracy w temperaturze 0-45 stopni Celcjusza |
| **Komponenty dodatkowe** | Wymagane jest dostarczenie komponentów kompatybilnych z przełącznikami i pochodzących od tego samego producenta co przełączniki: 1 x kabel Direct Attach 10GbE SFP+ o długości min. 0,5 metra. |
| **Gwarancja** | Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez telefon.Zamawiający przewiduje opcję w postaci możliwości wydłużenia terminu gwarancji wykonawcy lub producenta do pięciu lat na poniższych warunkach:* Przedłużenie gwarancji nastąpi na warunkach takich samych lub korzystniejszych dla Zamawiającego jak dla okresu podstawowego;
* Przedłużenie nastąpi o okres 2 lat względem okresu podstawowego (trzyletniego), co w konsekwencji spowoduje, iż pełen okres gwarancji wyniesie 5 lat od dnia odbioru przedmiotu zamówienia;
* Przedłużenie nastąpi automatycznie po jednostronnym oświadczeniu Zamawiającego skierowanym do Wykonawcy. Zamawiający ma obowiązek złożyć takie oświadczenie przed upływem podstawowego terminu gwarancji;
* Wykonawcy nie przysługuje roszczenie o wydłużenie okresu gwarancji;
* Wykonawcy przysługiwać będzie wynagrodzenie za dodatkowy okres gwarancji zgodne z treścią oferty i umowy;

Pozostałe warunki dotyczące realizacji zamówienia w zakresie opcji, zostały opisane we wzorze Umowy i SIWZ. |

## Przełączniki sieciowe typ 2 – 2 sztuki

| **Wymagania minimalne dla każdego przełącznika** |
| --- |
|  | Przełącznik FC musi być wykonany w technologii FC 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2 Gb/s z funkcją autonegocjacji prędkości. |
|  | Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 8 portów FC przełącznika.  |
|  | Przełącznik musi być dostarczony wraz z minimum 8 modułami SFP FC 8 Gb/s oraz 2 kablami LC-LC o dł. min. 5m. |
|  | Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
|  | Przełącznik FC musi posiadać nadmiarowe wentylatory N+1. |
|  | Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. |
|  | Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.  |
|  | Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. |
|  | Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. |
|  | Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:* Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric
* Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
* Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP
* Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów
* Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
* Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric.
* Konta użytkowników definiowane w środowisku RADIUS lub LDAP
* Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
* Obsługa SNMP v3
 |
|  | Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.  |
|  | Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. |
|  | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC |
|  | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1) |
|  | Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP |
|  | Maksymalny dopuszczalny pobór mocy przełącznika FC to 60W |
|  | Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. |
|  | Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns. |
|  | Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN |
|  | Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric. |
|  | Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). |
|  | Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
|  | Być objęty gwarancją na sprzęt przynajmniej na trzy lata.Gwarancja powinna być świadczona w trybie co najmniej 365x7x24, z czterogodzinnym czasem reakcji. |
|  | Produkt musi być fabrycznie nowy. |
|  | Szyny do montażu w szafie rack. |

## Macierz dyskowa typ 1 – 1 sztuka

|  |  |
| --- | --- |
|  | **Wymagania minimalne** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5”. |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów FC 16Gb wraz z wkładkami 4xSFP FC16Gb.  |
| **Cache** | 8GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. |
| **Dyski**  | Zainstalowane 17 dysków Hot-Plug SAS o pojemności 1.2TB SAS 10k RPM oraz 3 dyski 960GB SSD SAS RI 12Gbps, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| **Oprogramowanie / Funkcjonalności** | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| **Wsparcie dla systemów operacyjnych** | Zamawiający wymaga, aby macierz współpracowała z posiadanymi i użytkowanymi u Zamawiającego systemami operacyjnymi: Windows Server 2012 R2, Windows Server 2016, co najmniej dwa z rodziny Linux, Vmware ESXi, oraz oferowanym oprogramowaniem do wirtualizacji opisanym w punkcie 2.1.2. |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| **Warunki gwarancji dla macierzy** | Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez telefon. W przypadku awarii nośników pozostają one własnością Zamawiającego.Możliwość sprawdzenia statusu gwarancji poprzez stronę internetową po podaniu unikatowego numeru urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników.* Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
* Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
* W czasie obowiązywania gwarancji Wykonawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Certyfikaty** | Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2008 lub równoważną.  |

## Macierz dyskowa typ 2 – 1 sztuka

|  |  |
| --- | --- |
| **Parameter** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5”. |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów FC 16Gb wraz z wkładkami 4xSFP FC16Gb. |
| **Cache** | 8GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. |
| **Dyski**  | Zainstalowane 6 dysków Hot-Plug SAS o pojemności 8TB SAS 7.2k RPM 3,5”, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| **Oprogramowanie/Funkcjonalności** | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| **Wsparcie dla systemów operacyjnych** | Zamawiający wymaga, aby macierz współpracowała z posiadanymi i użytkowanymi u Zamawiającego systemami operacyjnymi: Windows Server 2012 R2, Windows Server 2016, co najmniej dwa z rodziny Linux, Vmware ESXi. oraz oferowanym oprogramowaniem do wirtualizacji opisanym w punkcie 2.1.2  |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| **Warunki gwarancji dla macierzy** | Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez telefon. W przypadku awarii nośników pozostają one własnością Zamawiającego.Możliwość sprawdzenia statusu gwarancji poprzez stronę internetową podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników.* Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
* Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
* W czasie obowiązywania gwarancji Wykonawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Certyfikaty** | Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2008 lub równoważną.  |

## Urządzenia zabezpieczające

Dla zapewnienia bezpieczeństwa inwestycji, w tym szybkiego wsparcia technicznego, pełnej kompatybilności sprzętu i wydajności systemu urządzeń zabezpieczających wymaga się, aby sprzęt UTM - pkt 1.7.1 niniejszego OPZ, sprzęt CPL – pkt 1.7.3 niniejszego OPZ oraz opcjonalnie sprzet WAF – pkt 1.7.2. niniejszego OPZ pochodził od jednego producenta.

### Sprzęt zabezpieczający klasy UTM (Unified Threat Management) – 1 sztuka

### Wymagania Ogólne

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

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

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

### Redundancja, monitoring i wykrywanie awarii

* W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
* W ramach postępowania system musi zostać dostarczony w postaci redundantnej (2 urządzenia w konfiguracji wysokiej dostępności).
* Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
* Monitoring stanu realizowanych połączeń VPN.
* System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

### Interfejsy, Dysk, Zasilanie

* System realizujący funkcję Firewall musi dysponować minimum:
	+ 8 portami Gigabit Ethernet RJ-45.
	+ 8 gniazdami SFP 1 Gbps.
	+ 2 gniazdami SFP+ 10 Gbps.
* System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
* W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
* System musi być wyposażony w zasilanie AC.

### Parametry wydajnościowe

* W zakresie Firewall’a obsługa nie mniej niż 7 mln jednoczesnych połączeń oraz 280.000 nowych połączeń na sekundę.
* Przepustowość Stateful Firewall: nie mniej niż 30 Gbps.
* Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps.
* Wydajność szyfrowania VPN IPSec nie mniej niż 10 Gbps.
* Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
* Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4,5 Gbps.
* Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 5 Gbps.

### Funkcje Systemu Bezpieczeństwa

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

* Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
* Kontrola Aplikacji.
* Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
* Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
* Ochrona przed atakami - Intrusion Prevention System.
* Kontrola stron WWW.
* Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
* Zarządzanie pasmem (QoS, Traffic shaping).
* Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
* Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
* Analiza ruchu szyfrowanego protokołem SSL.
* Analiza ruchu szyfrowanego protokołem SSH.

### Polityka Firewall

* Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
* System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.

- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

* W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

### Połączenia VPN

* System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
	+ Wsparcie dla IKE v1 oraz v2.
	+ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	+ Obsługa protokołu Diffie-Hellman grup 19 i 20.
	+ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
	+ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	+ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	+ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	+ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	+ Mechanizm „Split tunneling” dla połączeń Client-to-Site.
* System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
	+ Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
	+ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

### Routing i obsługa łączy WAN

* W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	+ Routingu statycznego.
	+ Policy Based Routingu.
	+ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
* System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

### Zarządzanie pasmem

* System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
* Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
* System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

### Kontrola Antywirusowa

* Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
* System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
* System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android, który jest najczęściej używanym systemem mobilnym u Zamawiającego).

### Ochrona przed atakami

* Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
* Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
* Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
* System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
* Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
* Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

### Kontrola aplikacji

* Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
* Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
* Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox – używane przez zamawiającego) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
* Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
* Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

### Kontrola WWW

* Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
* W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
* Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
* Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
* System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
* Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

### Uwierzytelnianie użytkowników w ramach sesji

* System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
	+ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
	+ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
	+ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
* Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
* Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

### Zarządzanie

* Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
* Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
* Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
* System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
* System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API. Wykonawca w ramach dostawy przekazuje dokumentację umożliwiającą podłączenie się do API.
* System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

### Logowanie

* System musi mieć możliwość logowania do systemu logowania i raportowania będącego przedmiotem postępowania.
* W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
* Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
* Musi istnieć możliwość logowania do serwera SYSLOG.

### Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.
* ICSA lub NSS Labs dla funkcji IPS.
* ICSA dla funkcji IPSec VPN.

### Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android, który jest najczęściej używanym systemem mobilnym u Zamawiającego), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

### Gwarancja oraz wsparcie

Sprzęt wraz z oprogramowaniem UTM, musi być objęty serwisem gwarancyjnym przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu Wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

### Uwagi dodatkowe i opcja

* W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca zapewnia, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.)
* Zamawiający przewiduje opcję w postaci możliwości zakupu drugiej sztuki sprzętu zabezpieczającego klasy UTM opisanego w niniejszym punkcie (pkt 1.7.1 OPZ) oraz umożliwiającego uruchomienie obu sztuk w trybie HA, w pełni kompatybilnego z oferowanym sprzętem klasy UTM oraz CPL i WAF (w przypadku skorzystania z prawa opcji na zakup sprzętu WAF), tj. sprzętu tego samego producenta, co zaoferowany sprzęt klasy UTM oraz CPL (i ewentualnie WAF). W przypadku skorzystania z opcji Wykonawca zobowiązany jest wykonać wdrożenie oraz inne usługi opisane w pkt 3 niniejszego OPZ odpowiednio dla przedmiotu opcji. Zamawiający zrealizuje opcję poprzez złożenie oświadczenia o woli skorzystania z opcji w postaci zlecenia dostawy całości lub części niżej opisanego sprzętu klasy UTM. Oświadczenie wraz ze zleceniem zakupu może być złożone Wykonawcy najpóźniej w ciągu 6 miesięcy od dnia zrealizowania i odebrania podstawowego zakresu zamówienia (bez elementów opisanych jako opcja). Termin realizacji zamówienia w ramach opcji: 5 tygodni od dnia przekazania oświadczenia o skorzystaniu z prawa opcji.

## Sprzęt zabezpieczający klasy WAF (Web Application Firewall) – 1 sztuka (opcja)

Zamawiający przewiduje opcję w postaci możliwości zakupu sprzętu klasy WAF (Web Application Firewall) opisanego w niniejszym punkcie (pkt 1.7.2 OPZ) w pełni kompatybilnego z oferowanym sprzętem klasy UTM oraz CPL, tj. sprzętu tego samego producenta, co zaoferowany sprzęt klasy UTM oraz CPL. W przypadku skorzystania z opcji Wykonawca zobowiązany jest wykonać wdrożenie oraz inne usługi opisane w pkt 3 niniejszego OPZ odpowiednio dla przedmiotu opcji. Zamawiający zrealizuje opcję poprzez złożenie oświadczenia o woli skorzystania z opcji w postaci zlecenia dostawy całości lub części niżej opisanego sprzętu klasy WAF. Oświadczenie wraz ze zleceniem zakupu może być złożone Wykonawcy najpóźniej w ciągu 6 miesięcy od dnia zrealizowania i odebrania podstawowego zakresu zamówienia (bez elementów opisanych jako opcja). Termin realizacji zamówienia w ramach opcji: 5 tygodni od dnia przekazania oświadczenia o skorzystaniu z prawa opcji. W ramach opcji możliwy będzie zakup sprzętu klasy WAF, opisanego w pkt 1.7.2 i poniżej.

### Wymagania Ogólne

System ochrony aplikacji webowych, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

### Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Powinna istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
3. Produkt nie powinien posiadać ograniczeń co do ilości chronionych aplikacji web.
4. Powinna istnieć możliwość zdefiniowania co najmniej 10 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
5. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive.

### Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi dysponować minimum:
* 3 portami Gigabit Ethernet RJ-45.
1. Powierzchnia dyskowa - minimum 240 GB typu SSD.
2. Zasilanie z sieci 230V/50Hz.
3. Obudowa urządzenia o wysokości do 1 U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

### Parametry wydajnościowe

1. Przepustowość dla ruchu http - min 90 Mbps.

### Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Tryb auto-uczenia – przyspieszający i ułatwiający implementację.
2. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
* Round Robin,
* Weighted Round Robin,
* Least Connection,
* Source IP Hash,
1. Wsparcie dla mechanizmów session persistence:
* Source IP
* HTTP Header
* URL parameter
* Insert Cookie
* Rewrite Cookie
* Persistent Cookie
* Embedded Cookie
* ASP Session ID
* PHP Session ID
* JSP Session ID
* SSL Session ID
1. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.1, TLS 1.2.
2. Możliwość analizy poszczególnych rodzajów ruchu w oparciu o polityki bezpieczeństwa (polityka to obiekt określający zbiór ustawień zabezpieczających aplikacje).
3. Ochrona aplikacji www przed takimi zagrożeniami jak:
* SQL and OS Command Injection.
* Cross Site Scripting (XSS).
* Cross Site Request Forgery.
* Outbound Data Leakage.
* HTTP Request Smuggling.
* Buffer Overflow.
* Encoding Attacks.
* Cookie Tampering / Poisoning.
* Session Hijacking.
* Broken Access Control.
* Forceful Browsing /Directory Traversal.
* Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP.
* DoS w warstwie aplikacji.
* Ochrona przed atakami typu Brute force.
* Ochrona przed atakami clickjacking.
* Ochrona przed credential stuffing.
1. Mechanizmy ochrony przed wyciekiem informacji poufnych.
2. Definiowanie polityk w oparciu o geo-lokalizację.
3. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
4. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.
5. Wsparcie dla ochrony http 2 natywnego oraz offload do http 1.1 w trybie pracy reverse proxy.
6. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only”.
7. Content routing na bazie parametrów http oraz certyfikatów X.509.
8. Ochrona przed Web Scraping.
9. Wsparcie dla kompresji danych oraz cache.
10. Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos).
11. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF.
12. Ochrona przed atakami typu SLOW (Slowloris i podobne).
13. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Wyłączanie konkretnych sygnatur na podstawie wielu parametrów: profil bezpieczeństwa:
* Metoda HTTP.
* IP klienta.
* Host.
* URI.
* Cały URL.
* Parametr.
* Cookie.
1. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.
2. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
3. Możliwość konfigurowania własnych stron z informacjami o błędzie.
4. Ustawienie wymaganej sekwencji otwieranych stron.
5. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML.
6. Detekcja XML w body żądań typu http POST w celu skutecznego użycia sygnatur do ochrony aplikacji web.
7. Detekcja JSON w żądaniach http w celu skutecznego użycia sygnatur do ochrony aplikacji web.
8. Blokowania „Illegal XML Format” oraz „Illegal JSON Format”.

### Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji http realizowana lokalnie lub na zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2. Skaner aplikacji WWW realizowany bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.
3. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.
4. Dekodowanie Base64 oraz CSS.
5. Domyślne szablony ochrony dla Exchange, SharePoint i WordPress – posiadanych i używanych przez Zamawiającego.
6. Uwierzytelnianie użytkowników w oparciu o protokół SAML.
7. Rozpoznawanie użytkowników logujących się bezpośrednio do chronionej aplikacji bez udziału WAF.
8. Wsparcie dla CAPTCHA do weryfikacji użytkowników.
9. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu od użytkowników generujących ataki z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa.

### Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.

### Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera syslog.
3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

### Certyfikaty

NSS Labs, ICSA Labs lub równoważne.

### Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem minimum w okresie gwarancyjnym.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
* Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 36 miesięcy.
* Aktualizacje skanera podatności aplikacji.

### Gwarancja oraz wsparcie

System WAF musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent lub Wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5. W przypadku wymiany urządzenia w ramach gwarancji, uszkodzone urządzenie pozostaje do dyspozycji Zamawiającego.

### Rozszerzone wsparcie serwisowe i uwagi dodatkowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez Wykonawcę, producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy lub infolinię w języku polskim 8x5.
3. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca zapewnia, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.).

## Centralny system logowania

### Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

### Interfejsy, Dysk, Zasilanie

1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45.
2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.

### 1.7.3.3 Parametry wydajnościowe

1. System musi być w stanie przyjmować minimum 90 GB logów na dzień.
2. System musi być w stanie analizować minimum 3000 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

**Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym z możliwością zastosowania filtrów dla prezentowanych informacji.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe - dla urządzeń, które logują informacje - obrazujące stan pracy urządzeń oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów, do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie VPN, utracone połączenie sieciowe, obciążenie zasobów.

**Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub Wykonawca musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

1. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

### 1.7.3.4 Gwarancja oraz wsparcie

Gwarancja: Centralny system logowania musi być objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent lub Wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5. W przypadku wymiany urządzenia w ramach gwarancji, uszkodzone urządzenie pozostaje do dyspozycji Zamawiającego.

### 1.7.3.5 Rozszerzone wsparcie serwisowe i uwagi dodatkowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora lub Wykonawcę przez okres 36 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.
3. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca zapewnia, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.).

## Komputer typu laptop

### Typ 1 – 2 sztuki

|  |  |
| --- | --- |
| Nazwa | Wymagane parametry techniczne |
| Zastosowanie | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Przekątna Ekranu | Komputer przenośny typu notebook z ekranem o przekątnej w przedziale 13" – 13,5’’ o rozdzielczości FHD (1920 x 1080) lub wyższą z podświetleniem LED i powłoką przeciwodblaskową, jasność minimum 300 nits, kontrast min. 600:1, maksymalny rozmiar plamki 0,154 mm |
| Procesor  | Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 7670 punktów Passmark CPU Mark.Zgodność z SIWZ będzie weryfikowana w oparciu o wynik testu dla oferowanego procesora dostępny na stronie : <https://www.cpubenchmark.net/cpu_list.php>  |
| Płyta główna | Wyposażona w dedykowany chipset dla oferowanego procesora..  |
| Pamięć RAM | 8GB DDR4 min. 2400MHz możliwość rozbudowy do min 16GB  |
| Pamięć masowa | 256GB M.2 PCIe SSD |
| Karta graficzna | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1000 punktów w G3D Rating, Zgodność z SIWZ będzie weryfikowana w oparciu o wynik testu dla oferowanej karty dostępny na stronie : <http://www.videocardbenchmark.net/gpu_list.php>  |
| Klawiatura | Klawiatura wyspowa w układzie QWERTY, z wbudowanym w klawiaturze podświetleniem (układ US -QWERTY), min 80 klawiszy. |
| Multimedia | Karta dźwiękowa zgodna z High Definition, wbudowane dwa głośniki stereo Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.Kamera internetowa z diodą informującą o aktywności, o rozdzielczości min. 1280x720, trwale zainstalowana w obudowie matrycy. czytnik kart micro SD, 1 port audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Karta sieci bezprzewodowej WiFi 802.11ac + bluetooth  |
| Bateria i zasilanie | Min. 7000 mAh] w technologii Li-lon. z zasilaczem umożliwiającym jej szybkie naładowanie do poziomu 80% w czasie do 1 godziny i do poziomu 100% w czasie do 2 godzin. |
| Waga i wymiary | Waga max 1,5kg z baterią  |
| Obudowa | Szkielet obudowy i zawiasy notebooka wykonane z metalu,.Kąt otwarcia notebooka min 180 stopni.  |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera, kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach.Funkcje BIOS:Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Możliwość włączenia/wyłączenia zintegrowanego kontrolera USB,Możliwość włączenia/wyłączenia dosilenia portu USB,Możliwość włączenia/wyłączenia zintegrowanego kontrolera audio,Możliwość włączenia/wyłączenia zintegrowanego mikrofonu,Możliwość włączenia/wyłączenia zintegrowanych głośników,Możliwość włączenia/wyłączenia szybkiego ładownia baterii.Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN– opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN,Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
| Certyfikaty | sprzęt wyprodukowany zgodnie z ISO9001:2000 oraz ISO 14001 lub normami równoważnymi.sprzęt posiada deklarację zgodności CE |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 19dB |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika, dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności:• testy uruchamiane automatycznie lub w trybie interaktywnym• możliwość powtórzenia testów• podsumowanie testów z możliwością zapisywania wyników• uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu,Uruchamianie testów zdefiniowanych przez użytkownika• wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów• wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera.Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o natywnej rozdzielczości matrycy, numerze seryjnym, typie i pojemności dysku twardego, o żywotności baterii – informacja podana w %, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość, obsadzenie w konkretnym banku, typ pamięci wraz z taktowanie oraz SN i PN, wykaz temperatur dla baterii, CPU, pamięci, temperatury panującej wewnątrz. |
| 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.Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy Czytnik SmartCard  |
| System operacyjny | Zainstalowany system operacyjny klasy PC musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez InternetDarmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat minimum do końca okresu gwarancyjnego); Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony internetowej. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne nieodpłatnie minimum w okresie gwarancji. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. . Wbudowany system pomocy w języku polskim; Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabowidzących); Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Wsparcie dla Oracle Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, posiadanych przez zamawiającego; Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem; Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową; Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; Graficzne środowisko instalacji i konfiguracji; Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe Udostępnianie modemu; Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; Możliwość przywracania plików systemowych; System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).. Możliwość zarządzania systemem operacyjnym za pomocą polityk domenowych usługi Microsoft Active Directory (w wersji 2008R2) – rozwiązanie wykorzystywane i zaimplementowane u Zamawiającego.System musi umożliwiać instalację i uruchomienie bez dodatkowej emulacji oprogramowania Sage Symfonia ERP 2019.1.d – wykorzystywanej przez Zamawiającego. |
| Porty i złącza | Wbudowane porty i złącza: 2x USB 3.1, 1x USB TYP-C Thunderbolt3, port zasilania |
| Warunki gwarancyjne | Firma serwisująca musi posiadać ISO 9001:2008 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.Minimalny czas trwania wsparcia technicznego wynosi 3 lata. Wydłużenie okresu gwarancji będzie punktowane w ramach jednego z kryteriów oceny ofert, zgodnie z opisem w SIWZ.Sposób realizacji usług wsparcia technicznego:Zgłaszanie usterek w dni robocze w godzinach 8-17 na adres e-mail. Skuteczne zgłoszenie polega na przesłaniu informacji o awarii na ustalony w umowie adres e-mail. .Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy lub technik serwisowy przybędzie na miejsce naprawy na następny dzień roboczy od momentu przyjęcia zgłoszenia.Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej.Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej również dla urządzeń z nieaktywnym wsparciem technicznym.Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii do serwisuW przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| Akcesoria | Dołączona dedykowana torba na laptopa |

### Typ 2 – 7 sztuk

|  |  |
| --- | --- |
| Nazwa | Wymagane parametry techniczne |
| Zastosowanie | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Przekątna Ekranu | Komputer przenośny typu notebook z ekranem 14" o rozdzielczościFHD (1920 x 1080) lub wyższej z podświetleniem LED i powłoką przeciwodblaskową, jasność min. 220 nits, kontrast min. 700:1, maksymalny rozmiar plamki 0,161 mm |
| Procesor  | Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 7450 punktów Passmark CPU Mark. Zgodność z SIWZ będzie weryfikowana w oparciu o wynik testu dla oferowanego procesora dostępny na stronie : <https://www.cpubenchmark.net/cpu_list.php>  |
| Płyta główna | Wyposażona w dedykowany chipset dla oferowanego procesora. |
| Pamięć RAM | 16GB DDR4 2400MHz możliwość rozbudowy do min 32GB, wymagane min. 2 sloty na pamięci, pracująca z procesorem na magistrali 2400MHz  |
| Pamięć masowa | 256GB PCIe NVMe SSD |
| Karta graficzna | Z możliwością dynamicznego przydzielenia pamięci systemowej. Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 900 punktów w G3D Rating. Zgodność z SIWZ będzie weryfikowana w oparciu o wynik testu dla oferowanego procesora dostępny na stronie : <http://www.videocardbenchmark.net/gpu_list.php>  |
| Klawiatura | Klawiatura wyspowa w układzie QWERTY, powłoka antybakteryjna, z wbudowanym w klawiaturze podświetleniem, (układ US -QWERTY), min 80 klawiszy. |
| Multimedia | Karta dźwiękowa zgodna z High Definition, wbudowane dwa głośniki stereo Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.Kamera internetowa z diodą informującą o aktywności, o rozdzielczości min. 1280x720, trwale zainstalowana w obudowie matrycy. czytnik kart SD, 1 port audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Karta sieci bezprzewodowej WiFi 802.11ac z dwoma antenami + bluetooth min. 4.1 |
| Bateria i zasilanie | Min. 68Wh z zasilaczem umożliwiającym jej szybkie naładowanie do poziomu 80% w czasie do 1 godziny i do poziomu 100% w czasie do 2 godzin. |
| Waga i wymiary | Waga max 2,3kg z baterią  |
| Obudowa | Szkielet obudowy i zawiasy notebooka wykonany z metalu,Kąt otwarcia notebooka min 180 stopni.  |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera, kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach.Funkcje BIOS:Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Możliwość włączenia/wyłączenia zintegrowanego kontrolera USB,Możliwość włączenia/wyłączenia dosilenia portu USB,Możliwość włączenia/wyłączenia zintegrowanego kontrolera audio,Możliwość włączenia/wyłączenia zintegrowanego mikrofonu,Możliwość włączenia/wyłączenia zintegrowanych głośników,Możliwość włączenia/wyłączenia szybkiego ładownia baterii.Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN– opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN,Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
| Certyfikaty | sprzęt wyprodukowany zgodnie z normą ISO9001:2000 lub równoważną oraz 140001 lub równoważnąDeklaracja zgodności CE |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 19dB |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika, dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności:• testy uruchamiane automatycznie lub w trybie interaktywnym• możliwość powtórzenia testów• podsumowanie testów z możliwością zapisywania wyników• uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu,Uruchamianie testów zdefiniowanych przez użytkownika• wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów• wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera.Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o natywnej rozdzielczości matrycy, numerze seryjnym, typie i pojemności dysku twardego, o żywotności baterii – informacja podana w %, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci, obsadzenie w konkretnym banku, typ pamięci wraz z taktowanie oraz SN i PN, wykaz temperatur dla baterii, CPU, pamięci, temperatury panującej wewnątrz. |
| 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.Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy Czytnik SmartCard  |
| System operacyjny | Zainstalowany system operacyjny klasy PC musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: * możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
* Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet;
* Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) minimum w okresie gwarancji;
* Internetowa aktualizacja zapewniona w języku polskim;
* Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
* Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
* Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi)
* Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
* Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać.
* Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
* Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
* Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
* Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie;
* Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
* Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
* Wbudowany system pomocy w języku polskim;
* Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabowidzących);
* Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
* Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
* Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
* System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
* Wsparcie dla Oracle Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, posiadanych przez Zamawiającego;
* Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
* Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;
* Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową;
* Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;
* Graficzne środowisko instalacji i konfiguracji;
* Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
* Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
* Udostępnianie modemu;
* Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
* Możliwość przywracania plików systemowych;
* System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
* Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

Możliwość zarządzania systemem operacyjnym za pomocą polityk domenowych usługi Microsoft Active Directory (w wersji 2008R2) – rozwiązanie wykorzystywane i zaimplementowane u Zamawiającego.System musi umożliwiać instalację i uruchomienie bez dodatkowej emulacji oprogramowania Sage Symfonia ERP 2019.1.d – wykorzystywanej przez Zamawiającego. |
| Porty i złącza | Wbudowane porty i złącza: 1x VGA, 1x HDMI 1.4, 1x RJ-45, 3x USB 3.1 w tym jeden port z zasilaniem, 1x USB TYP-C, port zasilania |
| Warunki gwarancyjne | Firma serwisująca musi posiadać ISO 9001:2008 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.Minimalny czas trwania wsparcia technicznego wynosi 3 lata. Wydłużenie okresu gwarancji będzie punktowane w ramach jednego z kryteriów oceny ofert, zgodnie z opisem w SIWZ.Sposób realizacji usług wsparcia technicznego:* Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17.
* Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi.

Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy lub technik serwisowy przybędzie na miejsce naprawy na następny dzień roboczy od momentu zgłoszenia awarii zgodnie z umową.Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej.Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej również dla urządzeń z nieaktywnym wsparciem technicznym minimum w trakcie trwania gwarancji.Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii do serwisuW przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| Akcesoria | Dołączona dedykowana torba do laptopa |

## Komputer typu stacjonarnego – 12 sztuk

|  |  |
| --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne komputerów |
| Typ | Komputer stacjonarny. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| Procesor  | Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 11 800 punktów. Zgodność z SIWZ będzie weryfikowana w oparciu o wynik testu dla oferowanego procesora dostępny na stronie: <https://www.cpubenchmark.net/cpu_list.php>. |
| Pamięć operacyjna RAM | 16GB DDR42400MHznon-ECC,możliwość rozbudowy do min 64GB |
| Parametry pamieci masowej | M.2 256 GB SSD SATAKomputer musi umożliwiać instalację min 3 HDD, dopuszcza się kombinację 1x SSD i 2 x dysk magnetyczny 3,5” i/lub 2,5” |
| Wydajność grafiki | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1050 punktów w G3D Rating. Zgodność z SIWZ będzie weryfikowana w oparciu o wynik testu dla oferowanej karty dostępny na stronie <http://www.videocardbenchmark.net/gpu_list.php> |
| Wyposażenie multimedialne | Min 24-bitowa Karta dźwiękowa, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. audio out. |
| Obudowa | Typu Small form factor z obsługą kart PCI Express wyłącznie o niskim profilu „LowProfile”, wyposażona w min. 1 wnękę wewnętrznie umożliwiającą montaż dysku 3,5” lub 2 dysków 2,5”. Napęd optyczny w dedykowanej wnęce zewnętrznej slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. Nie dopuszcza się, aby w bocznych ściankach obudowy były usytuowane otwory wentylacyjne, cyrkulacja powietrza tylko przez przedni i tylny panel z zachowaniem ruchu powietrza przód -> tył. Suma wymiarów obudowy nie może przekraczać 70cm, waga max 8 kgZasilacz 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, napędu optycznego, dysku 3,5” oraz 2,5”, bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych, śrub radełkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi być wyposażona w zamek szybkiego dostępu i musi być usytuowany na tylnym panelu.Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisk POWER [tzn. barw i miganie] w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej [w tym również portów I/O, chipset], awarię CMOS baterii, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych w specyfikacji wnęk zewnętrznych Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz musi być wpisany na stałe w BIOS. |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi. |
| Bezpieczeństwo | 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. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności: testy uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów. podsumowanie testów, uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu. wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów, wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów. Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera. Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, typ pamięci wraz z taktowanie oraz SN i PN, wykaz temperatur CPU, pamięci. System działający nawet w przypadku braku dysku twardego lub w przypadku jego uszkodzenia, pozwalający na uzyskanie wyżej wymienionych funkcjonalności a w szczególności na przetestowanie: procesora i pamięci. W przypadku braku możliwości uruchomienia graficznego systemu diagnostycznego komputer musi zawierać w sobie dodatkowo niezależny system diagnostyczny wizualny oparty o sygnalizację świetlną informujący użytkownika o awarii (system opisany przy obudowie). |
| Zdalne zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:* monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;
* zdalną konfigurację ustawień BIOS,
* zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;
* zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie;
* zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.
* technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/)
* nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS.
* wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego

sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji |
| 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). |
| BIOS | BIOS zgodny ze specyfikacją UEFI,Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). 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, dacie produkcji komputera, włączonej lub wyłączonej funkcji aktualizacji BIOS, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, aktywnym kanale – dual channel, 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, maksymalnej osiąganej prędkości zainstalowanego procesora, pamięci cache L2 zainstalowanego procesora, pamięci cache L3 zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dyskach twardych podpiętych do dostępnych na płycie głównej portów SATA oraz M.2, rodzajach napędów optycznych, MAC adresie zintegrowanej karty sieciowej, układzie graficznym lub zainstalowanym dedykowanym układzie graficznym, kontrolerze audio.Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo)Możliwość włączenia/wyłączenia kontrolera audio,Możliwość włączenia/wyłączenia układu TPM.Możliwość ustawienia czujnika obudowy w tryb cichy - nie informuje użytkownika o otwarciu obudowy (dźwiękiem i komunikatem) ale zapisuje log operacji. Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB,Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN– opcje do wyboru: tylko LAN, tylko WLAN, LANMożliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/OMożliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia dodatkowych funkcji sprzętowych Virtual Machine Mnitor (MVMM)Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Funkcja zbierania i zapisywania incydentów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę oraz opis incydentu kodu wizualnego systemu diagnostycznego. Funkcja pozwalająca na włączenie/wyłączenie automatycznego tworzenia recovery BIOS na dysku twardym lub na urządzeniu zewnętrznym podpiętym przez USBMożliwość wyłączania portów USB pojedynczo.Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min.: uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, wejścia do BIOS, upgrade BIOS bez konieczności uruchamiania systemu operacyjnego. Oraz dostępu do sieci LAN lub internetu, - dostęp do konsoli zaimplementowanej konsoli zarządzania zdalnego ( funkcja automatycznie aktywna w przypadku zaoferowania komputera z zdalnym zarządzaniem ) |
| Certyfikaty i standardy | sprzęt wyprodukowany zgodnie z normą ISO9001 lub równoważną oraz ISO 50001 lub równoważnąsprzęt posiada deklarację zgodności CE |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22 dB |
| Warunki gwarancji | Firma serwisująca musi posiadać ISO 9001:2008 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeńMinimalny czas trwania wsparcia technicznego wynosi 3 lata. Wydłużenie okresu gwarancji będzie punktowane w ramach jednego z kryteriów oceny ofert, zgodnie z opisem w SIWZ.Sposób realizacji usług wsparcia technicznego:* Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17.
* Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi.

Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy lub technik serwisowy przybędzie na miejsce naprawy na następny dzień roboczy od momentu zgłoszenia awarii zgodnie z umową.Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej.Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej., minimum w trakcje trwania okresu gwarancyjnegoDostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii do serwisuW przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| Wsparcie techniczne | Dostęp do najnowszych sterowników i uaktualnień na stronie internetowej. |
| System operacyjny | Zainstalowany system operacyjny klasy PC musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: * możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
* Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet;
* Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat), minimalnie w okresie gwarancyjnym;
* Internetowa aktualizacja zapewniona w języku polskim;
* Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
* Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
* Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
* Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać.
* Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
* Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
* Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
* Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie;
* Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
* Wbudowany system pomocy w języku polskim;
* Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabowidzących);
* Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
* Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
* Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
* System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
* Wsparcie dla Oracle Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, posiadanych i używanych obecnie w NIZP-PZH;
* Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
* Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;
* Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową;
* Rozwiązanie ma umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację;
* Graficzne środowisko instalacji i konfiguracji;
* Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
* Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
* Udostępnianie modemu;
* Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
* Możliwość przywracania plików systemowych;
* System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
* Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
* System powinien umożliwiać pełną instalację bez emulacji oprogramowania Sage Symfonia ERP 2018 użytkowanego przez Zamawiającego.

Możliwość zarządzania systemem operacyjnym za pomocą polityk domenowych usługi Microsoft Active Directory (w wersji 2008R2) – rozwiązanie wykorzystywane i zaimplementowane u Zamawiającego.System musi umożliwiać instalację i uruchomienie bez dodatkowej emulacji oprogramowania Sage Symfonia ERP 2019.1.d – wykorzystywanej przez Zamawiającego. |
| Wymagania dodatkowe | Wbudowane porty: 2x DisplayPort v1.1a 1x RS232,1x HDMI 2.02x PS/2, 1x LAN 10/100/1000 wspierająca obsługęWoL (funkcja włączana przez użytkownika), umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem.Porty USBPanel przedni- 4x USB w układzie 3x USB TYP A (1x USB 3.1 i 2x USB 2.0) i 1x USB TYP-C 3.1Panel Tylny- 6x USB TYP-A w układzie 4x USB 3.1 i 2x USB 2.0 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB TYP-A i TYP-C 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. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową (wlutowane w laminat płyty głównej).Płyta główna wyposażona w:1 złącza PCI Express x16 Gen.3, 1 złącza PCI Epress x 4, 4 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, 3 złącza SATA w tym 2 szt SATA 3.0; konfiguracja RAID 0/11 złącze M.2 2280 dedykowane dla syków M.2 SATA lub NVMe1 złącze M.2 WLAN1 konektor realizujący funkcję clear CMOS1 konektor realizujący funkcję clear PasswordKlawiatura USB w układzie polski programisty z czytnikiem kart inteligentnychMysz USB z rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |

## Monitor 24” – 12 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne monitora** |
| Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą IPS o przekątnej min. 23” |
| Rozmiar plamki (maksymalnie) | 0,275 mm x 0,275 mm |
| Jasność | min. 250 cd/m2 |
| Kontrast | min. 1000:1 |
| Kąty widzenia (pion/poziom) | 178/178 stopni |
| Czas reakcji matrycy(maksymalnie) | 5ms (gray to gray) w trybie fast8ms (gray to gray) w trybie normal |
| Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |
|  |  |
| Pochylenie monitora | wymagana możliwość regulacji pochylenia |
| Wydłużenie w pionie | wymagane, regulacja w zakresie min 130 mm |
| PIVOT | Tak |
| Obrót lewo/prawo | Min. 90 stopni |
| Powłoka powierzchni ekranu | Antyodblaskowa |
| Podświetlenie | System podświetlenia LED |
| Zużycie energii | maksymalne 45W, czuwanie poniżej 0,5 W |
| Bezpieczeństwo | Monitor musi być wyposażony w slot na linkę zabezpieczającą |
| Złącze  | 1x 15-stykowe złącze D-Sub, 1x HDMI (v1.4), 1x złącze DisplayPort (v1.2)2 x USB 3.0 (na bocznej ściance monitora)1 USB 3.0 port - upstream2 x USB 2.0 ports (w tylnej obudowie monitora) |
| Gwarancja | 3 lata na miejscu u klientaCzas reakcji serwisu - do końca następnego dnia roboczegoFirma serwisująca musi posiadać ISO 9001:2000 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputeraGwarancja zero martwych pikseli |
| Certyfikaty | sprzęt wyprodukowany zgodnie z: ISO 13406-2 lub ISO 9241 lub normami równoważnymi, Energy Star, TCO lub równoważnych. |
| Inne | Podstawa monitora umożliwiająca bezpośrednie umieszczenie i podłączenie oferowanego w niniejszym postępowaniu komputera stacjonarnego tworząca jeden zestaw |

## Urządzenie UPS dla komputerów stacjonarnych– 12 sztuk

1. Moc pozorna/rzeczywista: 650 VA/360 Watt
2. Architektura: Line-interactive
3. Maksymalny czas przełączania na baterię: 10 ms
4. Liczba i rodzaj gniazdek: 4 x IEC320 lub równoważna C13 (10 A)
5. Czas podtrzymania dla obciążenia 230 W /115W: 3 min/18 min
6. Zakres napięcia wejściowego: 170 – 260 V
7. Urządzenie musi zostać wyposażone w gniazdo USB, umożliwiające poprzez zainstalowane na PC oprogramowanie bezpiecznie zamknięcie oferowanego system operacyjnego w przypadku awarii zasilania

## Urządzenia UPS dla serwerów – 2 sztuki

|  |  |  |
| --- | --- | --- |
| Lp. | Parametr | Wartość |
|  | Moc | Co najmniej 3000VA /2700W |
|  | Współczynnik mocy | Co najmniej 0,9 |
|  | Tolerancja częstotliwości na wejściu | Przynajmniej 45 – 60Hz |
|  | Max Sprawność | Co najmniej 92% |
|  | Technologia | „On-line” |
|  | Wymiary, Dł. X Szer. X Wys. (mm) | Tower /Rack 19” wys. 2U max gł. 750mm |
|  | Zakres napięcia wejściowego AC | 160~270VAC  |
|  | THD wyj. | ≤ 2%  |
|  | Ochrona przed zwarciami  | TAK |
|  | By-pass  | TAK |
|  | Panel kontrolny | Graficzny |
|  | Komunikaty z panelu  | Wielofunkcyjna kontrola sterownicza i informacyjna |
|  | Alarm Praca z baterii | Charakterystyczny wyłącznie dla tego zdarzenia sygnał dźwiękowy |
|  | Alarm niski poziom baterii | Charakterystyczny wyłącznie dla tego zdarzenia sygnał dźwiękowy |
|  | Alarm Przeciążenie | Charakterystyczny wyłącznie dla tego zdarzenia sygnał dźwiękowy |
|  | Alarm Ogólny | Sygnał dźwiękowy ciągły |
|  | Komunikacja | RJ-45 10/100 Base-T, USB |
|  | Podwójne wejście zasilanie oddzielne dla toru By-pass, oddzielne dla toru prostownika | TAK |
|  | Złącze DC do dodatkowych baterii | TAK |
|  | Złącza wejściowe / wyjściowe  | Przynajmniej:2 x IEC-C19 lub wg normy równoważnej8 x IEC-C13 lub wg normy równoważnej |
|  | EPO | TAK |
|  | Naładowanie baterii do poziomu 80% | Poniżej 3h |
|  | Automatyczny restart po powrocie napięcia | TAK |
|  | Oprogramowanie  | zgodne z dostarczanymi dla serwerów systemami operacyjnymi |
|  | Poziom Hałasu | Poniżej 60dB |
|  | Zakres temperatur pracy | 0 do 40°C |
|  | Wyposażenie | Kabel USB, szyny montażowe, uchwyty do montażu w szafie 19” |
|  | Gwarancja | 3 lata standardowej gwarancji na urządzenie i akumulator. |
|  | Firmware | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu (najnowsza wersja firmware na dzień dostawy). |
|  | Norma CE | Urządzenia muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE. Dopuszcza się normy równoważne.  |
|  | Pochodzenie | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. |
|  | Identyfikacja | Urządzenia muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |
|  | Zasilanie | Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 200 V – 240 V, 50Hz. |

## 1.13 Urządzenie wielofunkcyjne – 2 szt.

|  |  |
| --- | --- |
| LP | Wymaganie |
| 1 | Laserowa technologia drukowania |
| 2 | Funkcja drukowania, kopiowania i skanowania, faksowania  |
| 3 | Możliwość druku czarno-białego i kolorowego |
| 4 | Możliwość druku jedno- i dwustronnego |
| 5 | Możliwość skanu jedno i dwustronnego |
| 6 | Kolorowy wyświetlacz LCD |
| 7 | Maksymalny rozmiar papieru A4 |
| 8 | Szybkość drukowania 2-stronnego co najmniej 6 obrazów na minutę |
| 9 | Standardowa szybkość drukowania A4 co najmniej 20 stron na minutę |
| 10 | Współpraca z komputerami PC z oferowanym systemem oraz systemami Windows 8, 8.1 oraz Windows 10 – używanymi przez Zamawiającego.  |
| 11 | Możliwość podłączenia do sieci przewodowej LAN |
| 12 | Możliwość podłączenia do sieci bezprzewodowej |
| 13 | Dodatkowy zestaw oryginalnych tonerów o standardowej pojemności: 1 x cyan, 1 x magenta, 1 x yellow, 1 x black |

# Oprogramowanie

## Oprogramowanie do wirtualizacji

### Oprogramowanie do wirtualizacji dla serwerów wskazanych w pkt 1.1

|  |  |
| --- | --- |
| 1 | Oferowane oprogramowanie musi być kompatybilne i nie może naruszać warunków licencyjnych posiadanego i użytkowanego oprogramowania Oracle Business Intelligence EE (OS.6. OBI EE), posiadanego przez Zamawiającego, odnośnie sposobu instalacji w oprogramowaniu wirtualizacyjnym. |
| 2 | **Wspierane systemy operacyjne (posiadane i wykorzystywane u Zamawiającego):*** **Oracle Linux , CentOS, Debian, Ubuntu**
* **Windows (7, 8, 8.1, 10)**
* **Windows Server (2003, 2008, 2012, 2016)**
 |
| 3 | Wysoka wydajność* Możliwość obsługi do 384 procesorów fizycznych
* Możliwość obsługi do 6TB pamięci RAM
* Możliwość przypisania do 256 vCPU per maszyna wirtualna
* Możliwość przypisania do 2TB pamięci RAM per maszyna wirtualna
 |
| 4 | Wysoka dostępność (HA) maszyn wirtualnych – w przypadku awarii serwera, system automatycznie uruchamia pracujące na nim maszyny wirtualne na innym serwerze. |
| 5 | Rozproszony harmonogram zasobów (DRS) |
| 6 | Rozproszone zarządzanie energią (DPM) |
| 7 | Możliwość migracji przestrzeni dyskowej na żywo (Storage Live Migration) |
| 8 | Możliwość migracji maszyn wirtualnych przy użyciu protokołu SSL (Secure Live Migration) |
| 9 | Możliwość klonowania zarówno zatrzymanych maszyn wirtualnych (cold cloning) jak i działających maszyn wirtualnych (hot cloning)  |
| 10 | Możliwość instalacji nowych środowisk wirtualnych z użyciem gotowych szablonów |
| 11 | Możliwość importowania oraz eksportowania maszyn wirtualnych w formatach Open Virtualization Format (OVF) oraz Open Virtualization Archive (OVA) |
| 12 | Możliwość aplikowania poprawek bezpieczeństwa bez potrzeby restartu wirtualizatora oraz maszyn wirtualnych  |
| 13 | Możliwość przypisania maszyn wirtualnych do wskazanych rdzeni procesora (hard partitioning) |
| 14 | Zapewnione wsparcie oprogramowania w okresie 3 lat. |

### Oprogramowanie do wirtualizacji dla serwerów wskazanych w pkt 1.2

|  |  |
| --- | --- |
| LP | Wymaganie |
|  |  |
| 1 | System do wirtualizacji z licencjami umożliwiającymi uruchamianie wirtualizacji na 3 serwerach fizycznych o łącznej liczbie minimum 6 procesorów fizycznych (2procesory per serwer) oraz jednej konsoli do zarządzania całym środowiskiem. Wirtualizacja musi umożliwić stworzenie klastra HA na dostarczonych serwerach. |
| 2 | Oprogramowanie musi być dostarczone z licencją uprawniającą do uruchomienia minimum dwóch środowisk wirtualnych.  |
| 3 | Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym. |
| 4 | Oprogramowanie do wirtualizacji musi umożliwiać klastrowanie zasobów obliczeniowych dostępnych na wielu serwerach fizycznych w celu lepszego wykorzystania tych zasobów do tworzenia maszyn wirtualnych. |
| 5 | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| 6 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 1TB pamięci operacyjnej. |
| 7 | Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 64 procesorów wirtualnych. |
| 8 | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności I dostępności pozostałych wybranych usług. |
| 9 | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| 10 | Rozwiązanie powinno wspierać co najmniej następujące systemy operacyjne: Windows Server 2012 R2, Debian, CentOS, Ubuntu posiadane przez Zamawiającego. |
| 11 | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| 12 | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi, usługami. Centralna konsola graficzna musi być dostępna minimum na systemy Windows, Mac i Linux |
| 13 | Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej. |
| 14 | Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych. |
| 15 | Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| 16 | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. |
| 17 | Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi. |
| 18 | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek. |
| 19 | System powinien posiadać funkcjonalność wirtualnego przełącznika (switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta. |
| 20 | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak, aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany. |
| 21 | Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych maszyn wirtualnych. |
| 22 | Rozwiązanie powinno zapewnić możliwość szybkiego tworzenia i uruchamiania nowych maszyn wirtualnych wraz z ich pełną konfiguracją i preinstalowanymi narzędziami systemowymi. |
| 23 | Licencja powinna być dostarczona wraz z 3 letnim wsparciem. |
| 24 | Oprogramowanie musi być zgodne z dostarczanym sprzętem opisanym w pkt 1.2 tj. oferowany sprzęt musi być wspierany przez producenta oprogramowania. |

## Oprogramowanie do obsługi kopii zapasowych (backupowania)

**Wymagania ogólne**

* Oprogramowanie musi współpracować z infrastrukturą oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez oferowane oprogramowanie do wirtualizacji opisane w punkcie 2.1.2 oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez oferowane oprogramowanie do wirtualizacji opisane w punkcie 2.1.2 i Hyper-V
* Licencja na oprogramowanie musi być dostarczona na min. 6 procesorów fizycznych wraz ze wsparcie producenta na poziomie podstawowym na okres minimum 3 lat

**Całkowite koszty posiadania**

* Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone
* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania, których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2 musi mieć możliwość aktualizacji pola typu „notatka” na wirtualnej maszynie
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) posiadanych przez Zamawiającego.
* Oprogramowanie musi zapewniać bezpośrednią integrację z oferowanym oprogramowaniem do wirtualizacji opisanym w punkcie 2.1.2i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

**Wymagania RPO**

* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
* Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
* Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2, pomiędzy hostami , włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

**Wymagania RTO**

* Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla srodowiska oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2 powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V stosowanego u Zamawiającego powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do powszechnie stosowanych platform chmurowych udostępnianych w modelu PaaS.
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć dla oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2 oraz PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	+ **Linux**
		- ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
		-
	+ **Windows**
		- NTFS, FAT, FAT32, ReFS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. używanych u Zamawiającego
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych używanych u Zamawiającego (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2014 i nowsze używane u Zamawiającego włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle używanych u Zamawiającego w celu szybkiego wyszukiwania plików w plikach backupowych.
* Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows używany u Zamawiającego używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku oferowanym oprogramowaniem do wirtualizacji opisanym w punkcie 2.1.2

**Monitoring**

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na oferowanym oprogramowaniu do wirtualizacji opisanym w punkcie 2.1.2 i Microsoft Hyper-V używanym u Zamawiającegobez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x, 6.0 oraz 6.5 używanych u Zamawiającego – przynajmniej w bezpłatnej wersji ESXi oraz oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 używanych u Zamawiającegozarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager używanych u Zamawiającego lub pracujące samodzielnie.
* System musi być przetestowany i certyfikowany przez oferowane oprogramowanie do wirtualizacji opisane w punkcie 2.1.2
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w oferowanym oprogramowaniu do wirtualizacji opisanym w punkcie 2.1.2
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
* System musi dawać możliwość podłączenia się do kilku instancji oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2 i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy oferowanej do wirtualizacji opisanej w punkcie 2.1.2
* System musi mieć możliwość monitorowania instancji oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2

**Raportowanie**

* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na oferowanym oprogramowaniu do wirtualizacji opisanym w punkcie 2.1.2 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2i 2016 posiadanego przez Zamawiającego.
* System musi wspierać wiele instancji oferowanego oprogramowania do wirtualizacji opisanym w punkcie 2.1.2 i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez oferowane oprogramowanie do wirtualizacji opisane w punkcie 2.1.2
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach oferowanego oprogramowania do wirtualizacji opisanego w punkcie 2.1.2 i Hyper-V
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy oferowanej do wirtualizacji opisanej w punkcie 2.1.2
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

# Wdrożenie i Usługi

|  |  |
| --- | --- |
| LP | Wymaganie dotyczące realizacji usług |
| 1 | Instalacja fizyczna w szafie rack 42U. Szafę zapewni Zamawiający |
| 2 | Podłączenie okablowania. Wykonawca dostarczy wszystkie niezbędne kable do prawidłowego połączenia dostarczanego w ramach niniejszego postępowania. Połączenia będą realizowane w ramach jednego pomieszczenia (punktu dystrybucyjnego/szafa Rack wymieniona w punkcie 1 niniejszej tabeli). W przypadku konieczności połączenia dostarczanego w niniejszym postępowaniu sprzętu w różnych pomieszczeniach/szafach rack Zamawiający we własnym zakresie zapewni odpowiednie okablowanie i połączenia pomiędzy tymi pomieszczeniami.  |
| 3 | Uruchomienie i sprawdzenie dostarczonego sprzętu  |
| 4 | Aktualizacja oprogramowania typu embeded / firmware |
| 5 | Konfiguracja sieci, zabezpieczeń |
| 6 | Instalacja systemów operacyjnych  |
| 7 | Instalacja i konfiguracja systemu wirtualizacji |
| 8 | Instalacja i konfiguracja systemu backupu |
| 9 | W przypadku konieczności prac mających wpływ na ciągłość działania Zamawiającego wymagane jest ich przeprowadzenie poza godzinami pracy Zamawiającego (16:30 – 07:00). |
| 10 | Wygenerowanie zasobów na macierzach i udostępnienie dla środowiska wirtualizacji na serwerach 1.1 i 1.2 |
| 11 | Przygotowanie dokumentacji powykonawczej |
| 12 | Przeszkolenie administratorów zamawiającego dla każdego z oferowanych rozwiązań w zakresie back-upu, monitoringu i wirtualizacji |
| 12.1 | Warsztat powinien trwać co najmniej 7 godzin i być przeprowadzony dla 3 osób |
| 12.2 | Warsztaty muszą być prowadzone poza siedzibą Zamawiającego |
| 12.3 | W przypadku ich realizacji w odległości większej niż 50km od siedziby Zamawiającego Wykonawca musi zapewnić nocleg dla uczestników oraz pokryć koszty dojazdu. |
| 13 | Konsultacje dla Zamawiającego w okresie 3 lat: |
| 13.1 | Telefoniczne – nie więcej niż 3h miesięcznie. |
| 13.2 | W lokalizacji – nie więcej niż 9 wizyt. |
| 13.3 | Wizyta trwa maksymalnie 6h |
| 14 | Podczas okresu trwania gwarancji Wykonawca zapewni wsparcie techniczne niezależne od producentów lub dystrybutorów oferowanych rozwiązań |
| 15. | Wsparcie ma obowiązywać w dni robocze w godzinach pracy Zamawiającego. |