***Załącznik 5a do OPZ – cz I zamówienia***

**Wymagania dla infrastruktury informatycznej**

w postępowaniu pn. Dostawa i wdrożenie sprzętu i oprogramowania

w ramach Projektu „Poprawa jakości i dostępności usług medycznych poprzez unowocześnienie systemu informatycznego w Zespole Opieki Zdrowotnej w Lidzbarku Warmińskim”

Spis treści

[I. Sprzęt IT 4](#_Toc90891613)

[1. Serwer aplikacyjny – 2 sztuki 4](#_Toc90891614)

[2. Serwer bazodanowy – 2 sztuki 7](#_Toc90891615)

[3. Serwer domenowy – 2 sztuki 11](#_Toc90891616)

[4. Macierz dyskowa – 1 sztuka 14](#_Toc90891617)

[5. Rozbudowa istniejącej macierzy 1 szt. 19](#_Toc90891618)

[6. Zasilacz UPS - 2 sztuki 20](#_Toc90891619)

[7. Przełącznik core – 1 sztuka 21](#_Toc90891620)

[8. Przełącznik dostępowy 48 portowy - 3 sztuki 23](#_Toc90891621)

[9. Przełącznik dostępowy 24 portowy (SWITCH – przełącznik sieciowy zarządzalny do montażu w szafie RACk 19’’)– 5 sztuk 25](#_Toc90891622)

[10. Przełącznik dostępowy 8 portowy – 3 sztuki 27](#_Toc90891623)

[11. Przełącznik dostępowy 48 portowy PoE – 3 sztuki 28](#_Toc90891624)

[12. Switch dla potrzeb serwerów (Przełącznik dostępowy 48 portowy) – 2 sztuki 30](#_Toc90891625)

[13. Punkt dostępowy AP – 38 sztuk 32](#_Toc90891626)

[14. Kontroler AP – 1 sztuka 33](#_Toc90891627)

[15. Firewall/UTM – 1 sztuka 35](#_Toc90891628)

[16. Duplikator z komputerem sterującym i monitorem 38](#_Toc90891629)

[1) Duplikator – 1 sztuka 38](#_Toc90891630)

[2) Komputer do duplikatora – 1 sztuka 38](#_Toc90891631)

[3) Monitor – 1 sztuka 44](#_Toc90891632)

[17. Stacja RTG - 1 komplet 45](#_Toc90891633)

[18. Rozmieszczenie sprzętu 47](#_Toc90891634)

[1) Serwer aplikacyjny – szt. 2 47](#_Toc90891635)

[2) Serwer bazodanowy – szt. 2 47](#_Toc90891636)

[3) Serwer domenowy – szt. 2 47](#_Toc90891637)

[4) Macierz dyskowa – szt. 1 47](#_Toc90891638)

[5) UPS – szt. 2 47](#_Toc90891639)

[6) Przełącznik CORE – szt. 2 47](#_Toc90891640)

[7) Switch dostępowy 48 – szt. 3 48](#_Toc90891641)

[8) Switch dostępowy 24 – szt. 5 48](#_Toc90891642)

[9) Switch dostępowy 8 – szt. 3 48](#_Toc90891643)

[10) Przełącznik dostępowy PoE – szt. 3 48](#_Toc90891644)

[11) Switch dla potrzeb serwerów – szt. 2 48](#_Toc90891645)

[12) Access Point (AP) – szt. 38 49](#_Toc90891646)

[13) Kontroler AP – szt. 1 50](#_Toc90891647)

[14) Firewall /UTM – szt. 1 50](#_Toc90891648)

[15) Duplikator z komputerem sterującym i monitorem – szt. 1 50](#_Toc90891649)

[16) Stacja RTG – szt. 1 50](#_Toc90891650)

[II. Oprogramowanie systemowe 51](#_Toc90891651)

[1. Oprogramowanie do backupu – 1 sztuka 51](#_Toc90891652)

[2. Systemy operacyjne serwerów 51](#_Toc90891653)

[1) Serwerowy system operacyjny dla potrzeb domeny – 2 sztuki 51](#_Toc90891654)

[2) Serwerowy system operacyjny dla potrzeb aplikacji oraz bazy danych – 4 sztuki 54](#_Toc90891655)

[3) Licencje dostępowe CAL – 150 sztuk 55](#_Toc90891656)

[3. Oprogramowanie do wirtualizacji – 1 komplet 55](#_Toc90891657)

[4. Oprogramowanie do zarządzania domeną 57](#_Toc90891658)

[1) Licencje oprogramowania do zarządzania siecią – 1 komplet 57](#_Toc90891659)

# Sprzęt IT

# Serwer aplikacyjny – 2 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | 1. Typu RACK, wysokość nie więcej niż 2U. 2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej. 3. Ramię porządkujące ułożenie przewodów z tyłu serwera. |
| **Płyta główna** | 1. Dwuprocesorowa. 2. Wyprodukowana i zaprojektowana przez producenta serwera. 3. Możliwość instalacji procesorów 28-rdzeniowych. 4. Zainstalowany moduł TPM 2.0. 5. 6 aktywnych złącz PCI Express generacji 3w tym: 6. 3 fizyczne złącza o prędkości x16, 7. 3 fizyczne złącza o prędkości x8, 8. Możliwość rozbudowy do 8 aktywnych złącz PCIe. 9. 24 gniazda pamięci RAM. 10. Obsługa minimum 3TB pamięci RAM. 11. Wsparcie dla technologii: 12. Memory Scrubbing, 13. SDDC, 14. Advanced ECC, 15. Rank Sparing, 16. Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM o pojemności sumarycznej minimum 1TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci), 17. Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug, |
| **Procesory** | 1. Dwa procesory 10-rdzeniowe, 2. architektura x86\_64   osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 119 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html |
| **Pamięć RAM** | 1. 128 GB pamięci RAM. 2. DDR4 Registered. 3. 2933Mhz. |
| **Dyski twarde i napędy** | 1. Minimum 4 wnęki dla dysków twardych Hotplug 3,5”. 2. Możliwość rozbudowy do 8 wnęk. 3. Możliwość instalacji dedykowanej wewnętrznej nagrywarki Blu-Ray. |
| **Kontrolery LAN** | 1. Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI oraz PXE boot. 2. Zainstalowana karta LAN 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 4x 10Gbit SFP+ bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express. |
| **Kontrolery I/O** | 1. Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe. 2. Zainstalowane dwa nośniki flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug. |
| **Porty** | 1. Zintegrowana karta graficzna ze złączami VGA z tyłu serwera. 2. 2 port USB 3.0 na panelu przednim. 3. 1 port USB wewnętrzny. 4. 2 porty USB 3.0 dostępne z tyłu serwera. 5. Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem. 6. Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. |
| **Zasilanie, chłodzenie** | 1. Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 800W. 2. Redundantne wentylatory hotplug. |
| **Zarządzanie** | 1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii): 2. informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:  * karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, * procesory CPU, * pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, * wbudowany na płycie głównej nośnik pamięci M.2 SSD, * status karty zrządzającej serwera, * wentylatory, * bateria podtrzymująca ustawienia BIOS płyty główne, * zasilacze,  1. system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym). 2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: 3. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera, 4. Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym, 5. Dostęp poprzez przeglądarkę Web, SSH, 6. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii, 7. Zarządzanie alarmami (zdarzenia poprzez SNMP), 8. Możliwość przejęcia konsoli tekstowej, 9. Możliwość zarządzania przez 6 administratorów jednocześnie, 10. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM), 11. Obsługa serwerów proxy (autentykacja), 12. Obsługa VLAN, 13. Możliwość konfiguracji parametru Max. Transmission Unit (MTU), 14. Wsparcie dla protokołu SSDP, 15. Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3, 16. Obsługa protokołu LDAP, 17. Integracja z HP SIM, 18. Synchronizacja czasu poprzez protokół NTP, 19. Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej. 20. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna). 21. Dedykowana, wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB. 22. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN. 23. Serwer musi posiadać możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. |
| **Wspierane OS** | 1. Microsoft Windows Server 2019, 2016. 2. VMWare vSphere 6.7. 3. Suse Linux Enterprise Server 12. 4. Red Hat Enterprise Linux 7, 8. 5. Univention Corporate Server 4. 6. Hyper-V Server. |
| **Gwarancja** | 1. 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera. 2. Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu. 3. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. 4. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie. |
| **Dokumentacja, inne** | 1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta. 2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta. 3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, 4. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. 5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera. |

# Serwer bazodanowy – 2 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | 1. Typu RACK, wysokość nie więcej niż 2U. 2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej. 3. Ramię porządkujące ułożenie przewodów z tyłu serwera. |
| **Płyta główna** | 1. Dwuprocesorowa. 2. Wyprodukowana i zaprojektowana przez producenta serwera. 3. Możliwość instalacji procesorów 28-rdzeniowych. 4. Zainstalowany moduł TPM 2.0. 5. 6 złącz PCI Express generacji 3 w tym: 6. 3 fizyczne złącza o prędkości x16, 7. 3 fizyczne złącza o prędkości x8, 8. Możliwość rozbudowy do 8 aktywnych złącz PCIe. 9. 24 gniazda pamięci RAM. 10. Obsługa minimum 3TB pamięci RAM. 11. Wsparcie dla technologii: 12. Memory Scrubbing, 13. SDDC, 14. Advanced ECC, 15. Rank Sparing. 16. Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM o pojemności sumarycznej minimum 1TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci). 17. Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug. |
| **Procesory** | 1. Jeden procesor 8-rdzeniowy (nie dopuszcza się większej ilości rdzeni fizycznych), 2. architektura x86\_64,   osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 109 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html |
| **Pamięć RAM** | 1. 192 GB pamięci RAM. 2. DDR4 Registered. 3. 2933Mhz. |
| **Dyski twarde i napędy** | 1. Minimum 4 wnęki dla dysków twardych Hotplug 3,5”. 2. Możliwość rozbudowy do 8 wnęk. 3. Możliwość instalacji dedykowanej wewnętrznej nagrywarki Blu-Ray. 4. Zainstalowane 3 dyski SAS 10k RPM Hot-Plug o pojemności 300GB. |
| **Kontrolery LAN** | 1. Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI oraz PXE boot. 2. Zainstalowana karta LAN 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 4x 10Gbit SFP+ bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express. |
| **Kontrolery I/O** | 1. Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe. 2. Zainstalowany kontroler RAID 0,1,1e,10,5,50. 3. Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug. |
| **Porty** | 1. Zintegrowana karta graficzna ze złączami VGA z tyłu serwera. 2. 2 port USB 3.0 na panelu przednim. 3. 1 port USB wewnętrzny. 4. 2 porty USB 3.0 dostępne z tyłu serwera. 5. Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem. 6. Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. |
| **Zasilanie, chłodzenie** | 1. Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 800W. 2. Redundantne wentylatory hotplug. |
| **Zarządzanie** | 1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii). 2. informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:  * karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, * procesory CPU, * pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, * wbudowany na płycie głównej nośnik pamięci M.2 SSD, * status karty zrządzającej serwera, * wentylatory, * bateria podtrzymująca ustawienia BIOS płyty główne, * zasilacze.  1. system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym). 2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: 3. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera, 4. Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym, 5. Dostęp poprzez przeglądarkę Web, SSH, 6. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii, 7. Zarządzanie alarmami (zdarzenia poprzez SNMP), 8. Możliwość przejęcia konsoli tekstowej, 9. Możliwość zarządzania przez 6 administratorów jednocześnie, 10. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM), 11. Obsługa serwerów proxy (autentykacja), 12. Obsługa VLAN, 13. Możliwość konfiguracji parametru Max. Transmission Unit (MTU), 14. Wsparcie dla protokołu SSDP, 15. Obsługa protokołów TLS 1.2, SSL v3, 16. Obsługa protokołu LDAP, 17. Integracja z HP SIM, 18. Synchronizacja czasu poprzez protokół NTP, 19. Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej. 20. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna). 21. Dedykowana, wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB. 22. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN. 23. Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. |
| **Wspierane OS** | 1. Microsoft Windows Server 2019, 2016. 2. VMWare vSphere 6.7. 3. Suse Linux Enterprise Server 12. 4. Red Hat Enterprise Linux 7, 8. 5. Univention Corporate Server 4. 6. Hyper-V Server. |
| **Gwarancja** | 1. 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana producenta serwera. 2. Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu. 3. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. 4. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie. |
| **Dokumentacja, inne** | 1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta. 2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta. 3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, 4. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. 5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; Dyski twarde nie podlegają zwrotowi organizacji serwisowej. |

# Serwer domenowy – 2 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | 1. Typu RACK, wysokość nie więcej niż 1U. 2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej. |
| **Płyta główna** | 1. Jednoprocesorowa. 2. Wyprodukowana i zaprojektowana przez producenta serwera. 3. Możliwość instalacji procesorów 8-rdzeniowych. 4. Zainstalowany moduł TPM 2.0. 5. 3 złącza PCI Express generacji 3, w tym: 6. 2 fizyczne złącza o prędkości x8, 7. 1 fizyczne złącze o prędkości x4, 8. Możliwość zainstalowania risera umożliwiającego instalację kart Full Height. 9. 4 gniazda pamięci RAM. 10. 4 zintegrowane porty SATA z możliwością konfiguracji RAID 0, 1, 10 oraz wsparciem dla systemów z rodziny Windows i Linux. 11. Wsparcie dla technologii: 12. Dual Channel, 13. ECC. |
| **Procesory** | 1. Procesor 6-rdzeniowy. 2. architektura x86. 3. Taktowanie 3,4GHz. 4. osiągający wynik Average CPU Mark 13800 pkt. Wynik musi być dostępny na stronie https://www.cpubenchmark.net. |
| **Pamięć RAM** | 1. 32 GB pamięci RAM. 2. DDR4 Registered. 3. 2666Mhz. 4. Możliwość rozbudowy do 128GB. |
| **Dyski twarde i napędy** | 1. Minimum 4 wnęki dla dysków twardych Hotplug 2,5”. 2. Możliwość rozbudowy do 8 wnęk. 3. Zainstalowane 4 szt. SSD SATA 6G 480GB HOT PLUG. |
| **Kontrolery LAN** | Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI, WoL oraz PXE boot. |
| **Kontrolery I/O** | 1. Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1 rozwiązanie dedykowane dla hypervisora, rozwiązanie niezajmujące zatok dla dysków hot-plug. 2. Zainstalowany kontroler RAID 0, 1, 1e, 10, 5, 50. |
| **Porty** | 1. Zintegrowana karta graficzna ze złączem VGA z tyłu serwera, możliwość zamontowania dedykowanego portu VGA z przodu serwera. 2. 2 porty USB 3.1 Gen 1 na panelu przednim. 3. 2 porty USB 2.0 dostępne z tyłu serwera. 4. 2 porty USB 3.1 Gen 2 dostępne z tyłu serwera. 5. Port serial. 6. Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. |
| **Zasilanie, chłodzenie** | 1. Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej nie większej niż 460W. 2. Redundantne wentylatory hotplug. |
| **Zarządzanie** | 1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; 2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: 3. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera, 4. Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; 5. Dostęp poprzez przeglądarkę Web, SSH, 6. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii, 7. Zarządzanie alarmami (zdarzenia poprzez SNMP), 8. Możliwość przejęcia konsoli tekstowej, 9. Możliwość zarządzania przez 6 administratorów jednocześnie, 10. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM), 11. Obsługa serwerów proxy (autentykacja), 12. Obsługa VLAN, 13. Możliwość konfiguracji parametru Max. Transmission Unit (MTU), 14. Wsparcie dla protokołu SSDP, 15. Obsługa protokołów TLS 1.2, SSL v3, 16. Obsługa protokołu LDAP, 17. Integracja z HP SIM, 18. Synchronizacja czasu poprzez protokół NTP, 19. Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej. 20. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna). 21. Zainstalowana dedykowana (lub zintegrowana) pamięć flash o pojemności minimum 16 GB; Pamięć umożliwiająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN oraz umożliwiającej możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. 22. Możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu. |
| **Wspierane OS** | 1. Microsoft Windows Server 2019, 2016. 2. VMWare vSphere 6.7, 6.5. 3. Suse Linux Enterprise Server 12. 4. Red Hat Enterprise Linux 7. |
| **Gwarancja** | 1. 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. 2. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych. 3. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie. |
| **Dokumentacja, inne** | 1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta. 2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta. 3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera. 4. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. 5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; Dyski twarde nie podlegają zwrotowi organizacji serwisowej. 6. Możliwość wykonania aktualizacji BIOS z nośnika USB. |

# Macierz dyskowa – 1 sztuka

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Ogólne** | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 4U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug NL-SAS,SSD oraz 3U/4U dla 60 dysków typu hotplug NL-SAS, SSD-SAS; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 24 HDD 2,5” + 12 HDD 3,5 + 60HDD). |
| **Pojemność** | 1. 56,5 TB realizowana na dyskach NL-SAS 12G 8TB (RAID-6 + Hot-spare). 2. 11,2 TB realizowana na dyskach SAS 12G 1,8TB (RAID-5 + Hot-spare). |
| **Kontrolery** | 1. Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. 2. Każdy z kontrolerów macierzy musi posiadać po minimum 64 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu. 3. Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD. 4. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk. 5. Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia. 6. Kontrolery macierzy obsługują funkcjonalność kompresji danych. 7. Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line. 8. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. 9. Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. 10. Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami. 11. Kontrolery macierzy muszą obsługiwać do 130 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów. 12. Oferowana macierz musi mieć wyprowadzone 2 porty iSCSI 10Gb/s LC MMF oraz 2 porty iSCSI 1Gb/s RJ-45 do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID. 13. Macierz musi umożliwiać wymianę portów do transmisji danych obsługujących protokoły: 14. 4 x FC 16Gb/s, 15. 2 x FC 16Gb/s, 16. 2 x FC 32Gb/s, 17. 2 x SAS 12GB/s 18. Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych. 19. Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS I NFS musi odbywać się jednocześnie – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy. |
| **Poziomy RAID** | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:   1. Raid-0, 2. Raid-1, 3. Raid-10, 4. Raid-5, 5. Raid-50, 6. Raid-6. |
| **Dyski** | 1. Oferowana macierz musi wspierać dyski hot-plug: 2. dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s, 3. dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm. 4. Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania. 5. Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex. 6. Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami. 7. Możliwość rozbudowy oferowanego modelu macierzy do minimum 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski. 8. Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy): 9. Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID, 10. Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID. 11. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess). 12. Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS i HDD-SAS/NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą. |
| **Opcje programowe** | 1. Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych. 2. Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN). 3. Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC. 4. Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów. 5. Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania I bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową. 6. Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere. 7. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI. 8. Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. 9. Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy. 10. Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’. 11. Macierz musi obsługiwać adresację IP v.4 i IP v.6. 12. Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji. 13. Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. 14. Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy. 15. Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania I sterowników. 16. Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN. 17. Macierz musi wspierać rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy. 18. Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN: 19. Sama deduplikacja wybranego LUN, 20. Sama kompresja wybranego LUN, 21. Kombinacja technologii kompresji i deduplikacji wybranego LUN, 22. Brak użycia technologii kompresji i deduplikacji dla wybranego LUN. |
| **Zarządzanie** | 1. Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej. 2. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 3. Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora. 4. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. |
| **Gwarancja i serwis** | 1. Całe rozwiązanie musi być objęte minimum 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowanym czasem skutecznego zakończenia naprawy najpóźniej w ciągu następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. 2. Dyski twarde nie podlegają zwrotowi organizacji serwisowej. 3. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. 4. Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 24 miesięcy. 5. System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy. 6. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych. 7. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia. 8. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). 9. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia. |

# Rozbudowa istniejącej macierzy 1 szt.

Zamawiający dopuszcza zamiast rozbudowy istniejącej macierzy, dostawę i instalację dwóch identycznych macierzy opisanych w pkt. 4.

|  |  |
| --- | --- |
| **L.p.** | **Opis wymagań** |
|  | Dedykowana półka dyskowa do posiadanej macierzy Eternus DX100 S5   1. elementy umożliwiające montaż w szafie RACK, 2. elementy umożliwiające redundantne podłączenie do posiadanej macierzy, 3. Zainstalowane 9 dysków SAS 12G 1,8TB 10 000 RPM, 4. 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia, 5. Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej, 6. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych, |
|  | Przedłużenie wsparcia gwarancyjnego do posiadanej macierzy Eternus DX100 S5:   1. Dodatkowy okres wsparcia gwarancyjnego producenta, aby jego koniec przypadał za 36 miesięcy od momentu dostawy, 2. Gwarancja skutecznego zakończenia naprawy w następnym dniu roboczym od skutecznego zgłoszenia. |
|  | Rozbudowa funkcjonalności posiadanej macierzy Eternus DX100 S5   1. o 4 dodatkowe interfejsy iSCSI 10Gb LC MMF (po dwa na kontroler), 2. licencja umożliwiająca uruchomienie replikacji synchronicznej i asynchronicznej wraz z 36-miesięcznym wsparciem producenta. |

# Zasilacz UPS - 2 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Technologia** | On-line. |
| **Moc** | Pozorna 3 kVA, rzeczywista 2,7kW. |
| **Obudowa** | 1. Zajętość w szafie RACK nie więcej niż 2U. 2. Moduł bateryjny dedykowany do UPS-a – zajętość w szafie nie więcej niż 2U. 3. Należy dostarczyć elementy umożliwiające montaż UPS-a oraz modułu bateryjnego w szafie RACK. |
| **Wyjścia na UPS-ie** | 1. 8 x IEC 320 C13 (10A). 2. 1 x RJ45 (karta SNMP). |
| **Oprogramowanie** | 1. Aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania. 2. Wspierane i certyfikowane systemy operacyjne: Microsoft Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware Infrastructure, Citrix XenServer. 3. Zarządzanie przez SNMP. |
| **Wyświetlacz** | Wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia. |
| **Moduł bateryjny** | Dodatkowy moduł bateryjny wydłużając czas podtrzymania zasilania do:   1. podtrzymanie 3,8 minuty przy 100% obciążeniu, 2. podtrzymanie 11,5 minuty przy 50% obciążeniu. |
| **Inne** | 1. Automatyczny wewnętrzny bypass. 2. Bezprzerwowa wymiana baterii. |
| **Certyfikaty** | CE, CB. |
| **Gwarancja** | 36 miesięcy gwarancji door-to-door. |

# Przełącznik core – 1 sztuka

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Klasa produktu** | SWITCH – przełącznik sieciowy zarządzalny do montażu w szafie RACK 19’’. |
| **Ogólne** | Obsługa warstwy trzeciej. |
| **Złącza** | 1. 10/100/1000Base-T (RJ45) - 8 szt. 2. 1000/10GBase-X (SFP+) - 24 szt. 3. 40GBase-X (QSFP) - 2 szt. |
| **Wydajność** | 1. Matryca Przełączająca: 656 Gb/s. 2. Przepustowość: 488 Mp/s. 3. bufor: 4MB. 4. Ramki Jumbo: 16k. 5. Tablica adresów MAC współdzielona dla unicast oraz multicast (w proporcji 1:1): 32k. 6. Maksymalna ilość adresów MAC – Multicast: 4k. 7. Tablica ACL: 3k. 8. Tablica Routingu współdzielona dla IPv4 oraz IPv6 (w proporcji 4:1): 16k. 9. Tablica ARP: 16k. 10. Ilość Interfejsów Vlan (IP): 1024. |
| **Dostępność** | 1. IEEE 802.1D STP/802.1w RSTP/802.1s MSTP. 2. IEEE 802.3ad LACP. 3. Virtual Cable Testing. 4. DDM. 5. LLDP / LLDP-MED. 6. VRRP. 7. Loop guard. 8. ERPS (ITU-T G.8032). |
| **Kontrola ruchu** | 1. 802.1Q VLAN (4K), Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN. 2. Voice VLAN, Mac VLAN, Super VLAN. 3. Algorytm LACP adresu IP/MAC źródłowego/docelowego (load balance). 4. GVRP. 5. 802.1ad Vlan Stacking (QinQ). 6. Flexible QinQ. |
| **Bezpieczeństwo** | 1. Layer 2 MAC filtering. 2. BPDU Tunnel. 3. Uwierzytelnienie i autoryzacja logowania poprzez RADIUS oraz TACACS+. 4. TACACS+ accounting/auditing. 5. SSH v1/v2. 6. DHCP/DHCPv6 snooping. 7. P/IPv6 Source Guard. 8. Port security. 9. IEEE 802.1x port-based / mac-based. |
| **QoS** | 1. 802.1p Priority Queues per Port: 8. 2. 802.1p Queuing method. 3. Trusted COS/TOS/IP Precedence/DSCP/Port number. 4. Broadcast Storm Control. 5. Rate Limiting, port based. 6. Strict priority, Strict priority in WDRR. 7. WRR, WDRR, WRED. |
| **L2/L3 - Multicast** | 1. Multicast VLAN. 2. IGMP v1,v2, v3. 3. IGMP Query. 4. IGMP Snooping (v1,v2,v3). 5. IGMP Snooping Fast Leave(v2,v3). 6. PIM-DM/SM/SSM. 7. anycast RP. 8. IPv6 MLD v1/v2 Snooping. |
| **Trasowanie** | 1. RIP v1,v2. 2. OSPF v2. 3. IPv6 Static Route. 4. RIPng. 5. OSPFv3. 6. BGP4+. 7. Warstwa 3 IPv6. 8. IPv4/IPv6 Dual Protocol Stack. 9. IPv6 address/ IPv6 Tunneling |
| **Zarządzanie** | Port Konsolowy:   1. GUI, 2. Zarządzanie poprzez port konsolowy, telnet, SNMP v1/v2c/v3, 3. TFTP/FTP, 4. Wielopoziomowy CLI. |
| **Inne** | 1. DNS Client. 2. DHCP Client/Server/Relay. 3. DHCP option 43/60/82. 4. DHCPv6 option 37/ 38. 5. DHCPv6 Relay/Server. 6. NTP. 7. RSPAN. 8. ERSPAN. 9. Cluster. 10. Stack (VSF). 11. OAM EFM IEEE 802.3ah. 12. OAM CFM IEEE 802.1ag. |
| **Akcesoria** | 1. Kompatybilne z przełącznikiem wkładki 10G SFP+ (na światłowód wielomodowy) – 8 sztuk. 2. Kompatybilne z przełącznikiem wkładki 1G SFP (na światłowód wielomodowy) – 8 sztuk. |
| **Gwarancja** | 1. Lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. 2. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

# Przełącznik dostępowy 48 portowy - 3 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Klasa produktu** | SWITCH – przełącznik sieciowy zarządzalny do montażu w szafie RACK 19’’. |
| **Ogólne** | Obsługa warstwy trzeciej. |
| **Złącza** | 1. 10/100/1000Base-T (RJ45) 48 szt. 2. 1000/10GBase-X (SFP+) - 4 szt. 3. Port zarządzający OOB (10/100Base-T RJ45) - 1 szt. |
| **Wydajność** | 1. Matryca Przełączająca: 176 Gb/s. 2. Przepustowość: 131 Mp/s. 3. bufor: 3MB, dopuszczalny 2x1,5MB. 4. Ramki Jumbo: 10k. 5. Tablica adresów MAC współdzielona dla unicast oraz multicast (w proporcji 1:1): 16k. 6. Maksymalna ilość adresów MAC – Multicast: 4k. 7. Tablica ACL: 1,4k. 8. Tablica Routingu współdzielona dla IPv4 oraz IPv6 (w proporcji 4:1): 1k. 9. Tablica ARP: 4k. 10. Ilość Interfejsów Vlan (IP): 1k. |
| **Dostępność** | 1. IEEE 802.1D STP/802.1w RSTP/802.1s MSTP. 2. IEEE 802.3ad LACP. 3. Virtual Cable Testing. 4. DDM. 5. LLDP / LLDP-MED. 6. VRRP. 7. Loop guard. 8. ERPS (ITU-T G.8032). |
| **Kontrola ruchu** | 1. 802.1Q VLAN (4K), Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN. 2. Voice VLAN, Mac VLAN, Super VLAN. 3. Algorytm LACP adresu IP/MAC źródłowego/docelowego (load balance). 4. GVRP. 5. 802.1ad Vlan Stacking (QinQ). 6. Flexible QinQ. |
| **Bezpieczeństwo** | 1. Layer 2 MAC filtering. 2. BPDU Tunnel. 3. Uwierzytelnienie i autoryzacja logowania poprzez RADIUS oraz TACACS+. 4. TACACS+ accounting/auditing. 5. SSH v1/v2. 6. DHCP/DHCPv6 snooping. 7. IP/IPv6 Source Guard. 8. Port security. 9. IEEE 802.1x port-based / mac-based. |
| **QoS** | 1. 802.1p Priority Queues per Port: 8. 2. 802.1p Queuing method. 3. Trusted COS/TOS/IP Precedence/DSCP/Port number. 4. Broadcast Storm Control. 5. Rate Limiting, port based. 6. Strict priority, Strict priority in WDRR. 7. WDRR, WRED. |
| **L2/L3 - Multicast** | 1. Multicast VLAN. 2. IGMP v1,v2, v3. 3. IGMP Query. 4. IGMP Snooping (v1,v2,v3). 5. IGMP Snooping Fast Leave(v2,v3). 6. PIM-DM/SM/SSM. 7. anycast RP. 8. IPv6 MLD v1/v2 Snooping. |
| **Routing** | 1. RIP v1,v2/ RIPng. 2. Routing statyczny IPv4/IPv6. 3. OSPF v2/ OSPFv3. 4. IPv6 Static Route. 5. BGP4+. 6. Warstwa 3 IPv6. 7. IPv4/IPv6 Dual Protocol Stack. 8. IPv6 address/ IPv6 Tunneling. |
| **Zarządzanie** | Port Konsolowy RS-232 (RJ45):   1. GUI, 2. Zarządzanie poprzez port konsolowy, telnet, SNMP v1/v2c/v3, 3. TFTP/FTP, 4. Wielopoziomowy CLI, 5. Kopia zapasowa konfiguracji oraz jej przywracanie. |
| **Inne** | 1. DNS Client. 2. DHCP Client/Server/Relay. 3. DHCP option 43/60/82. 4. DHCPv6 option 37/ 38. 5. DHCPv6 Relay/Server. 6. SNTP / NTP. 7. sFlow. 8. RSPAN. 9. ERSPAN. 10. Cluster. 11. Stack (VSF). 12. OAM EFM IEEE 802.3ah. 13. OAM CFM IEEE 802.1ag. |
| **Akcesoria** | 1. Kompatybilne z przełącznikiem wkładki 10G SFP+ (na światłowód wielomodowy) – 2 sztuki. 2. Kompatybilne z przełącznikiem wkładki 1G SFP (na światłowód wielomodowy) – 2 sztuki. |
| **Gwarancja** | 1. Lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. 2. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

# Przełącznik dostępowy 24 portowy (SWITCH – przełącznik sieciowy zarządzalny do montażu w szafie RACk 19’’)– 5 sztuk

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Ogólne** | Obsługa warstwy trzeciej |
| **Złącza** | 1. 10/100/1000Base-T (RJ45) 24 szt. 2. 1000/10GBase-X (SFP+) 4 szt. 3. Port zarządzający OOB (10/100Base-T RJ45) - 1 szt. |
| **Wydajność** | 1. Matryca Przełączająca: 128 Gb/s. 2. Przepustowość: 95 Mp/s. 3. bufor: 1,5MB. 4. Ramki Jumbo: 10k. 5. Tablica adresów MAC współdzielona dla unicast oraz multicast (w proporcji 1:1): 16k. 6. Maksymalna ilość adresów MAC – Multicast: 4k. 7. Tablica ACL: 1,4k. 8. Tablica Routingu współdzielona dla IPv4 oraz IPv6 (w proporcji 4:1): 1k. 9. Tablica ARP: 4k. 10. Ilość Interfejsów Vlan (IP): 1k. |
| **Dostępność** | 1. IEEE 802.1D STP/802.1w RSTP/802.1s MSTP. 2. IEEE 802.3ad LACP. 3. Virtual Cable Testing. 4. DDM. 5. LLDP / LLDP-MED. 6. VRRP. 7. Loop guard. 8. ERPS (ITU-T G.8032). |
| **Kontrola ruchu** | 1. 802.1Q VLAN (4K), Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN. 2. Voice VLAN, Mac VLAN, Super VLAN. 3. Algorytm LACP adresu IP/MAC źródłowego/docelowego (load balance). 4. GVRP. 5. 802.1ad Vlan Stacking (QinQ). 6. Flexible QinQ. |
| **Bezpieczeństwo** | 1. Layer 2 MAC filtering. 2. BPDU Tunnel. 3. Uwierzytelnienie i autoryzacja logowania poprzez RADIUS oraz TACACS+. 4. TACACS+ accounting/ auditing. 5. SSH v1/v2. 6. DHCP/DHCPv6 snooping. 7. P/IPv6 Source Guard. 8. Port security. 9. IEEE 802.1x port-based / mac-based. |
| **QoS** | 1. 802.1p Priority Queues per Port: 8. 2. 802.1p Queuing method. 3. Trusted COS/TOS/IP Precedence/DSCP/Port number. 4. Broadcast Storm Control. 5. Rate Limiting, port based. 6. Strict priority, Strict priority in WDRR. 7. WDRR, WRED. |
| **L2/L3 - Multicast** | 1. Multicast VLAN. 2. IGMP v1,v2, v3. 3. IGMP Query. 4. IGMP Snooping (v1,v2,v3). 5. IGMP Snooping Fast Leave(v2,v3). 6. PIM-DM/SM/SSM. 7. anycast RP. 8. IPv6 MLD v1/v2 Snooping. |
| **Routing** | 1. RIP v1,v2/ RIPng. 2. Routing statyczny IPv4/IPv6. 3. OSPF v2/ OSPFv3. 4. IPv6 Static Route. 5. BGP4+. 6. Warstwa 3 IPv6. 7. IPv4/IPv6 Dual Protocol Stack. 8. IPv6 address/ IPv6 Tunneling. |
| **Zarządzanie** | Port Konsolowy RS-232 (RJ45):   1. GUI, 2. Zarządzanie poprzez port konsolowy, telnet, SNMP v1/v2c/v3, 3. TFTP/FTP, 4. Wielopoziomowy CLI, 5. Kopia zapasowa konfiguracji oraz jej przywracanie. |
| **Inne** | 1. DNS Client. 2. DHCP Client/Server/Relay. 3. DHCP option 43/60/82. 4. DHCPv6 option 37/ 38. 5. DHCPv6 Relay/Server. 6. SNTP / NTP. 7. sFlow. 8. RSPAN. 9. ERSPAN. 10. Cluster. 11. Stack (VSF). 12. OAM EFM IEEE 802.3ah. 13. OAM CFM IEEE 802.1ag. |
| **Akcesoria** | 1. Kompatybilne z przełącznikiem wkładki 10G SFP+ (na światłowód wielomodowy) – 2 sztuki. 2. Kompatybilne z przełącznikiem wkładki 1G SFP (na światłowód wielomodowy) – 2 sztuki. |
| **Gwarancja** | 1. Lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. 2. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

# Przełącznik dostępowy 8 portowy – 3 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Klasa produktu** | SWITCH - przełącznik sieciowy zarządzalny do montażu w szafie RACK 19’’. |
| **Porty przełącznika:** | minimum 8 portów 10/100/1000Base-T, minimum 2 porty 1GE SFP. |
| **Zarządzanie:** | TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMPv1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Ping, Trace Route, Radius Authentication, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files. |
| **Szybkość przełączania:** | minimum 20 Gbps. |
| **Przepustowość:** | minimum 15 Mpps (dla pakietów 64Kb). |
| **Tablica adresów MAC** | minimum 8k . |
| **Ilość aktywnych IEEE802.1Q VLAN:** | minimum 4092. |
| **Obsługa VLAN:** | IEEE 802.1Q, QinQ, selektywne QinQ, elastyczne QinQ. |
| **Obsługa protokołów IP** | IPv4 oraz IPv6. |
| **Obsługa spanning tree:** | IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunel. |
| **Funkcje QoS:** | Klasyfikacja ruchu w oparciu o ACL, VLAN ID, Flow Redirect. |
| **Bezpieczeństwo:** | Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius, TACACS+. |
| **Multicast:** | IGMP v1/v2/v3 snooping, IGMP fast leave, MLD v1/v2 snooping, MVR, IPv4/IPv6 DCSCM(D). |
| **Zasilanie:** | zabudowany zasilacz 230V AC. |
| **Wkładki** | Kompatybilne z przełącznikiem wkładki 1G SFP (na światłowód wielomodowy) – 2 sztuki. |
| **Gwarancja:** | Lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

# Przełącznik dostępowy 48 portowy PoE – 3 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Klasa produktu** | SWITCH – przełącznik sieciowy zarządzalny do montażu w szafie RACK 19’’. |
| **Ogólne** | Obsługa warstwy trzeciej. |
| **Złącza** | 1. 10/100/1000Base-T (RJ45) PoE - 48 szt. 2. 1000/10GBase-X (SFP+) - 4 szt. 3. Port zarządzający OOB (10/100Base-T RJ45) - 1 szt. |
| **Wydajność** | 1. Matryca Przełączająca: 176 Gb/s. 2. Przepustowość: 131 Mp/s. 3. bufor: 3MB, dopuszczalny 2x1,5MB. 4. Ramki Jumbo: 10k. 5. Tablica adresów MAC współdzielona dla unicast oraz multicast (w proporcji 1:1): 16k. 6. Maksymalna ilość adresów MAC – Multicast: 1k. 7. Tablica ACL: 380. 8. Tablica Routingu współdzielona dla IPv4 oraz IPv6 (w proporcji 4:1): 512. 9. Tablica ARP: 512. 10. Ilość Interfejsów Vlan (IP): 512. |
| **Dostępność** | 1. IEEE 802.1D STP/802.1w RSTP/802.1s MSTP. 2. IEEE 802.3ad LACP. 3. Virtual Cable Testing. 4. DDM. 5. LLDP / LLDP-MED. 6. VRRP. 7. Loop guard. 8. ERPS (ITU-T G.8032). |
| **Kontrola ruchu** | 1. 802.1Q VLAN (4K), Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN. 2. Voice VLAN, Mac VLAN, Super VLAN. 3. Algorytm LACP adresu IP/MAC źródłowego/docelowego (load balance). 4. GVRP. 5. 802.1ad Vlan Stacking (QinQ). 6. Flexible QinQ. |
| **Bezpieczeństwo** | 1. Layer 2 MAC filtering. 2. BPDU Tunnel. 3. Uwierzytelnienie i autoryzacja logowania poprzez RADIUS oraz TACACS+. 4. TACACS+ accounting/auditing. 5. SSH v1/v2. 6. DHCP/DHCPv6 snooping. 7. IP/IPv6 Source Guard. 8. Port security. 9. IEEE 802.1x port-based / mac-based. |
| **QoS** | 1. 802.1p Priority Queues per Port: 8. 2. 802.1p Queuing method. 3. Trusted COS/TOS/IP Precedence/DSCP/Port number. 4. Broadcast Storm Control. 5. Rate Limiting, port based. 6. Strict priority, Strict priority in WDRR. 7. WDRR, WRED. |
| **L2/L3 - Multicast** | 1. Multicast VLAN. 2. IGMP v1,v2, v3. 3. IGMP Query. 4. IGMP Snooping (v1,v2,v3). 5. IGMP Snooping Fast Leave(v2,v3). 6. PIM-DM/SM/SSM. 7. anycast RP. 8. IPv6 MLD v1/v2 Snooping. |
| **Routing** | 1. RIP v1,v2/ RIPng. 2. Routing statyczny IPv4/IPv6. 3. OSPF v2/ OSPFv3. 4. IPv6 Static Route. 5. BGP4+. 6. Warstwa 3 IPv6. 7. IPv4/IPv6 Dual Protocol Stack. 8. IPv6 address. |
| **Zarządzanie** | Port Konsolowy RS-232 (RJ45):   1. GUI, 2. Zarządzanie poprzez port konsolowy, telnet, SNMP v1/v2c/v3, 3. TFTP/FTP, 4. Wielopoziomowy CLI, 5. Kopia zapasowa konfiguracji oraz jej przywracanie. |
| **Inne** | 1. DNS Client. 2. DHCP Client/Server/Relay. 3. DHCP option 43/60/82. 4. DHCPv6 option 37/ 38. 5. DHCPv6 Relay/Server. 6. SNTP / NTP. 7. sFlow. 8. RSPAN. 9. Cluster. 10. Stack (VSF). 11. OAM EFM IEEE 802.3ah. 12. OAM CFM IEEE 802.1ag. |
| **Zasilanie:** | 1. 230V AC zasilacz wbudowany w urządzenie, redundantne zasilanie 52-58 V DC. 2. PoE z budżetem mocy minimum 740W. |
| **Akcesoria** | Kompatybilne z przełącznikiem wkładki 10G SFP+ (na światłowód wielomodowy) – 2 sztuki. |
| **Gwarancja** | 1. Lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. 2. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

# Switch dla potrzeb serwerów (Przełącznik dostępowy 48 portowy) – 2 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Klasa produktu** | SWITCH – przełącznik sieciowy zarządzalny do montażu w szafie RACK 19’’. |
| **Ogólne** | Obsługa warstwy trzeciej. |
| **Złącza** | 1. 10/100/1000Base-T (RJ45) 48 szt. 2. 1000/10GBase-X (SFP+) - 4 szt. 3. Port zarządzający OOB (10/100Base-T RJ45) - 1 szt. |
| **Wydajność** | 1. Matryca Przełączająca: 176 Gb/s. 2. Przepustowość: 131 Mp/s. 3. bufor: 3MB, dopuszczalny 2x1,5MB. 4. Ramki Jumbo: 10k. 5. Tablica adresów MAC współdzielona dla unicast oraz multicast (w proporcji 1:1): 16k. 6. Maksymalna ilość adresów MAC – Multicast: 4k. 7. Tablica ACL: 1,4k. 8. Tablica Routingu współdzielona dla IPv4 oraz IPv6 (w proporcji 4:1): 1k. 9. Tablica ARP: 4k. 10. Ilość Interfejsów Vlan (IP): 1k. |
| **Dostępność** | 1. IEEE 802.1D STP/802.1w RSTP/802.1s MSTP. 2. IEEE 802.3ad LACP. 3. Virtual Cable Testing. 4. DDM. 5. LLDP / LLDP-MED. 6. VRRP. 7. Loop guard. 8. ERPS (ITU-T G.8032). |
| **Kontrola ruchu** | 1. 802.1Q VLAN (4K), Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN. 2. Voice VLAN, Mac VLAN, Super VLAN. 3. Algorytm LACP adresu IP/MAC źródłowego/docelowego (load balance). 4. GVRP. 5. 802.1ad Vlan Stacking (QinQ). 6. Flexible QinQ. |
| **Bezpieczeństwo** | 1. Layer 2 MAC filtering. 2. BPDU Tunnel. 3. Uwierzytelnienie i autoryzacja logowania poprzez RADIUS oraz TACACS+. 4. TACACS+ accounting/ auditing. 5. SSH v1/v2. 6. DHCP/DHCPv6 snooping. 7. P/IPv6 Source Guard. 8. Port security. 9. IEEE 802.1x port-based / mac-based. |
| **QoS** | 1. 802.1p Priority Queues per Port: 8. 2. 802.1p Queuing method. 3. Trusted COS/TOS/IP Precedence/DSCP/Port number. 4. Broadcast Storm Control. 5. Rate Limiting, port based. 6. Strict priority, Strict priority in WDRR. 7. WDRR, WRED. |
| **L2/L3 - Multicast** | 1. Multicast VLAN. 2. IGMP v1,v2, v3. 3. IGMP Query. 4. IGMP Snooping (v1,v2,v3). 5. IGMP Snooping Fast Leave(v2,v3). 6. PIM-DM/SM/SSM. 7. anycast RP. 8. IPv6 MLD v1/v2 Snooping. |
| **Routing** | 1. RIP v1,v2/ RIPng. 2. Routing statyczny IPv4/IPv6. 3. OSPF v2/ OSPFv3. 4. IPv6 Static Route. 5. BGP4+. 6. Warstwa 3 IPv6. 7. IPv4/IPv6 Dual Protocol Stack. 8. IPv6 address/ IPv6 Tunneling. |
| **Zarządzanie** | Port Konsolowy RS-232 (RJ45):   1. GUI. 2. Zarządzanie poprzez port konsolowy, telnet, SNMP v1/v2c/v3. 3. TFTP/FTP. 4. Wielopoziomowy CLI. 5. Kopia zapasowa konfiguracji oraz jej przywracanie. |
| **Inne** | 1. DNS Client. 2. DHCP Client/Server/Relay. 3. DHCP option 43/60/82. 4. DHCPv6 option 37/ 38. 5. DHCPv6 Relay/Server. 6. SNTP / NTP. 7. sFlow. 8. RSPAN. 9. ERSPAN. 10. Cluster. 11. Stack (VSF). 12. OAM EFM IEEE 802.3ah. 13. OAM CFM IEEE 802.1ag. |
| **Akcesoria** | 1. Kompatybilne z przełącznikiem wkładki 10G SFP+ (na światłowód wielomodowy) – 2 sztuki. 2. Kompatybilne z przełącznikiem wkładki 1G SFP (na światłowód wielomodowy) – 2 sztuki. |
| **Gwarancja** | 1. Lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. 2. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat. |

# Punkt dostępowy AP – 38 sztuk

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Parametry ogólne** | 1. Urządzenie sieciowe, punkt dostępowy dwuradiowy, w zamkniętej architekturze przeznaczone do montażu na ścianie, suficie podwieszanym lub suficie trwałym (z pomocą dodatkowych akcesoriów). 2. Urządzenie musi być w 100% kompatybilne z wyspecyfikowanym kontrolerem sieci bezprzewodowej. 3. Minimum 2 porty 10/100/1000Base-T. 4. Minimum 1 port USB 2.0. 5. Złącze zasilacza: 12V DC. 6. Możliwość pracy w trybie z kontrolerem (FIT), jak również w trybie samodzielnym (FAT). 7. Równoczesna praca na częstotliwościach 2.4 GHz oraz 5 GHz. 8. Komunikacja bezprzewodowa MIMO 4x4. |
| **Zasilanie** | Power over Ethernet IEEE 802.3at (pobór mocy max. 18W). |
| **Anteny** | wbudowane anteny 2.4 GHz zysk minimum 4dBi, wbudowane anteny 5GHz zysk minimum 5dBi. |
| **Wymagane tryby i częstotliwości pracy radia** | 802.11a/n : 5.150 GHz do 5.850 GHz 802.11b/g/n : 2.4 GHz do 2.483 GHz 802.11ac: 5.150GHz do 5.250GHz 5.250GHz do 5.350GHz 5.725GHz to 5.850GHz wave2. |
| **Wymagane obsługiwane technologie modulacji** | 802.11b: BPSK, QPSK, CCK 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM. |
| **Moc nadajnika radiowego (moc wyjściowa na złączu antenowym)** | 2,4GHz: 23 dBm (per Chain) 5GHz: 23 dBm (per Chain). |
| **Obsługa wirtualnych punktów dostępowych (BSSID)** | minimum 48 jednocześnie. |
| **Ilość obsługiwanych strumieni przestrzennych** | 2,4GHz: 2 oraz dla 5GHz: 4. |
| **Obsługa łączności bezprzewodowej** | Dynamiczna regulacja kanału (DCA), Kontrola mocy transmisyjnej (TPC), Wykrywanie i redukcja obszaru martwego, Ukryte SSID,RTS/CTS, Skanowanie środowiska RF, Dostęp hybrydowy, Ograniczenie dostępu dla liczby użytkowników, Kontrola integralności łącza, Ograniczenie dostępu do terminali ze słabymi sygnałami, Wymuszony roaming terminali ze słabymi sygnałami, Inteligentne przełączanie klientów zgodnie z Airtime Fairness, Optymalizacja aplikacji o wysokiej gęstości. |
| **Funkcje bezpieczeństwa** | Enkrypcja 64/128 WEP, TKIP oraz CCMP, 802.11i, WAPI, Autentykacja MAC adresu, Autentykacja LDAP, Autentykacja PEAP, WIDS/WIPS, Ochrona widma w czasie rzeczywistym, Ochrona przeciwko atakom DoS, Bezpieczeństwo przekierowań, Izolacja użytkowników, Okresowe włączanie i wyłączanie SSID, Kontrola dostępu do wolnych zasobów, Zabezpieczenie kontroli dostępu do terminali bezprzewodowych, Sprawdzanie poprawności adresu źródłowego (SAVI), ACL, Zabezpieczona kontrola dostępu do punków dostępowych. |
| **Funkcje sieciowe** | Konfiguracja statycznego adresu IP lub przydział adresu przez dynamiczny DHCP, Przekierowania IPv6, Portal IPv6, Lokalne przekierowania, Transmisja Multicast, Roaming, Warunki przełączania punktów dostępowych, WDS. |
| **Obsługa funkcji QoS (jakości usługi)** | WMM, Mapowanie priorytetów, Mapowanie polityki QoS, Filtrowanie pakietów L2-L4 i klasyfikacja przepływu, Równoważenie obciążenia, Limit przepustowości, Kontrola przyjęć połączeń (CAC), Tryb oszczędzania energii, Automatyczny mechanizm awaryjny punktów dostępowych, Inteligentna identyfikacja terminali, Konwersja transmisji multicast do transmisji unicast. |
| **Zarządzanie** | Scentralizowane zarządzanie poprzez kontroler; tryby pracy “fit” oraz ‘fat”, Konserwacja zdalna oraz lokalna, Lokalne logi, Syslog oraz logi eksportowane do pliku, Alarm, Wykrywanie uszkodzeń, Przełączanie pomiędzy trybami “fit” oraz “fat”, Zdalna analiza sondy, Dual-image (dual-OS), Watchdog. |
| **Stopień ochrony urządzenia** | IP41. |
| **Wilgotność:** | 10% do 90% (bez kondensacji). |
| **Temperatura pracy:** | 0°C do +50°C. |
| **Gwarancja** | Minimum 36 miesięcy. |

# Kontroler AP – 1 sztuka

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Parametry ogólne** | 1. Urządzenie sieciowe w zamkniętej architekturze o wysokości nie większej niż 1U. 2. Minimum 16x GE combo ports (GE/SFP), 2x GE SFP ports, 2x 1/10G Base X SFP+. 3. Minimum 1 port szeregowy konsoli (interfejs RJ-45). 4. Możliwość jednoczesnej obsługi minimum 256 punktów dostępowych. 5. Możliwość jednoczesnej obsługi minimum 10 000 użytkowników bezprzewodowych w sieci. 6. Obsługa jednocześnie do 4000 wirtualnych sieci VLAN zgodnych z IEEE 802.1Q. |
| **Pojemność tablicy MAC** | Minimum 16 000 wpisów. |
| **Pojemność tablicy ARP** | Minimum 4 000 wpisów. |
| **Obsługa funkcji L2** | IEEE802.1Q (VLAN), IEEEE802.1d (STP), IEEEE802.1W (RSTP), IEEEE802.1S (MSTP), IEEE802.1p (COS), IEEE802.1x (Port Control), IEEE802.3x (Flow Control), IEEE802.3ad (LACP), Port Mirror, IGMP Snooping, MLD Snooping, QinQ, GVRP, PVLAN, Broadcast control. |
| **Obsługa funkcji L3** | Static Routing, RIPv1/v2, OSPF, VRRP, IGMP v1/v2/v3, ARP, ARP Proxy, PIM-SM, PIM-DM, PIM-SSM. |
| **Protokoły i standardy Wireless** | 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11d, 802.11h, 802.11i, 802.11e, 802.11k. |
| **Obsługa protokołów IPv6 dla potrzeb przyszłościowego wykorzystania sieci** | IPv4/v6 dual-stack, DHCPv6, DNSv6, ICMPv6, ACLv6, TCP/UDP for IPv6, SOCKET for IPv6, SNMP v6, Ping /Traceroute v6, RADIUS, Telnet/SSH v6, FTP/TFTP v6, NTP v6, IPv6 MIB support for SNMP, VRRP for IPv6, static routing, OSPFv3, IPv6 SAVI. |
| **Współpraca z jednostką wysokiej dostępności (HA Unit)** | N+1 backup, N+N backup, Portal 1+1 backup, DHCP server backup. |
| **Zarządzanie funkcjami radiowymi punktów dostępowych** | Ustawianie kodów krajowych, Ręczne / automatyczne ustawianie mocy nadawania, Ręczne / automatyczne ustawianie kanału roboczego, Automatyczna regulacja szybkości transmisji, Wykrywanie i naprawa obszaru martwego, Skanowanie środowiska RF, które umożliwia punktom dostępowym skanowanie otaczającego środowiska RF, Wykrywanie i unikanie zakłóceń RF 11n-preferowana polityka RF, Ukryte SSID, Konfiguracja pasma kanału 20 MHz i 40 MHz, Ochrona czasu antenowego w dostępie hybrydowym terminali 11bg i 11n, Terminale w oparciu o harmonogram Airtime Fairness, Analiza spektralna, Lokalizacja terminala, Nawigacja widmowa (preferowana 5 GHz), 11n, limit liczby użytkowników w oparciu o SSID lub radio, Wykrywanie użytkownika online, Automatyczne wylogowanie użytkowników bez ruchu, Zakaz dostępu dla klientów o słabych sygnałach, Zdalna analiza sondy, Wymuszony roaming klientów ze słabymi sygnałami. |
| **Funkcje bezpieczeństwa** | 64/128 WEP, dynamiczny WEP, TKIP, CCMP; Uwierzytelnianie zabezpieczeń 802.11i oraz dwa tryby (Enterprise i Personal) 802.1x i PSK; Szyfrowanie i uwierzytelnianie WAPI; Uwierzytelnianie LDAP; Autentykacja adresów MAC; Uwierzytelnianie portalu, w tym wbudowany portal, portal zewnętrzny i portal niestandardowy; tryby uwierzytelniania; Uwierzytelnianie użytkownika PEAP; Przekazywanie kontroli bezpieczeństwa, takie jak filtrowanie ramek, biała lista, statyczna czarna lista i dynamiczna czarna lista; Izolacja użytkownika; Okresowe włączanie i wyłączanie radia / SSID; Kontrola dostępu do wolnych zasobów; Bezpieczna kontrola dostępu do terminali bezprzewodowych; Kontrola dostępu do różnych pakietów danych - IPv4 i IPv6 oraz MAC adresów; Bezpieczeństwo kontroli dostępu do punktów dostępowych: uwierzytelnianie MAC; uwierzytelnianie hasła; Klient Radius; Serwer kopii zapasowych autentykacji; Sprawdzanie poprawności adresu źródłowego (SAVI); Kontrola dostępu użytkowników na podstawie lokalizacji punktów dostępowych; Bezprzewodowy system wykrywania włamań (WIDS) i bezprzewodowy system zapobiegania włamaniom (WIPS); Ochrona przeciw zalewaniu portów (flooding attack); Ochrona przeciw podszywaniu się (spoofing attack). |
| **Obsługa roamingu** | Szybki roaming L2 / L3 pomiędzy punktami dostępowymi obsługiwanymi przez ten sam kontroler; Wymuszony roaming klientów ze słabymi sygnałami; Szybki roaming L2 / L3 pomiędzy punktami dostępowymi obsługiwanymi przez różne kontrolery. |
| **Obsługa funkcji QoS (jakości usługi)** | 802.11e (WMM); Port Ethernet 802.1P, identyfikacja i znakowanie; Mapowanie z priorytetów transmisji bezprzewodowej na priorytety transmisji przewodowe; Mapowanie różnych SSID / VLAN do różnych zasad QoS; Mapowanie strumieni danych, które pasują do różnych pól pakietów do różnych zasad QoS; Równoważenie obciążenia na podstawie liczby użytkowników, ruchu oraz pasm częstotliwości; Limit przepustowości na podstawie punktów dostępowych, identyfikatorów SSID, terminali oraz określonych strumieni danych; Tryb oszczędzania energii; Konwersja transmisji multicast do transmisji unicast. |
| **Funkcje zarządzania** | Zarządzanie poprzez Web; Konfiguracja przez port konsolowy; SNMP v1/v2c/v3; Konserwacja lokalna i zdalna; Lokalne dzienniki zdarzeń, Syslog i eksport logów do pliku; Statystyki; Logowanie poprzez Telnet; Logowanie poprzez SSH; Dual-image (dual-OS); Sprzętowy Watchdog; zarządzanie klastrem kontrolerów; automatyczna synchronizacja informacji pomiędzy kontrolerami, a klastrem oraz automatyczne lub ręczne przekazanie informacji konfiguracyjnych; SSID oparte na mechanizmie zarządzania uprawnieniami użytkownikami. |
| **Wilgotność:** | 5% do 90% (bez kondensacji). |
| **Temperatura pracy:** | 0°C do +55°C. |
| **Zasilanie** | Wbudowany zasilacz 230V AC, maksymalny pobór mocy 25W. |
| **Gwarancja** | Minimum 36 miesięcy. |

# Firewall/UTM – 1 sztuka

|  |  |
| --- | --- |
| **L.p.** | **Wymagane minimalne parametry techniczne** |
|  | Zapora sieciowa typu Next Generation Firewall (NGFW). |
|  | Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku. |
|  | Minimalna ilość interfejsów:   1. 4 interfejsy 2.5 GbE SFP, 2. 4 interfejsy 2.5 GbE, 3. 12 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa, 4. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G, 5. 1 interfejs konsoli do zarządzania zaporą, 6. 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą. |
|  | Zapora musi posiadać dysk SSD o pojemności przynajmniej 16 GB z możliwością wymiany na większy. |
|  | Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa. |
|  | Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji. |
|  | Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q. |
|  | Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej. |
|  | Minimalna ilość jednocześnie obsługiwanych połączeń: 1 000 000. |
|  | Możliwość obsłużenia przynajmniej 14 000 nowych połączeń w ciągu 1 sekundy. |
|  | Przepustowość urządzenia pracującego w trybie stateful firewall: 3 Gbps – dla ramki 1518B zgodnie z RFC 2544. |
|  | Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.4 Gbps. |
|  | Przepustowość urządzenia pracującego jako koncentrator VPN: 1.45 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544. |
|  | Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 1 000. |
|  | Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000. |
|  | Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne. |
|  | Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 300 Mbps oraz obsłużyć 60 000 połączeń. |
|  | Obsługa IPSec, ISAKMP/IKE, Radius, PPPoE, PPTP. |
|  | Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site). |
|  | Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa). |
|  | Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP. |
|  | Wsparcie dla Dynamicznego DNS tzw. DDNS. |
|  | Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne. |
|  | Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio). |
|  | Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:   1. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, 2. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. |
|  | Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL. |
|  | Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. |
|  | Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN). |
|  | Kontrola dostępności zestawionych tuneli VPN. |
|  | Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty. |
|  | Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić). |
|  | Funkcja NAT oparta o reguły bezpieczeństwa. |
|  | NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe). |
|  | Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych. |
|  | Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www. |
|  | Funkcja NAT oparta o reguły bezpieczeństwa. |
|  | NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe). |
|  | Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych. |
|  | Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www. |
|  | System IPS musi używać algorytmu szeregowego przetwarzania. |
|  | Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex). |
|  | Systemy skanowania IPS/Antywirus muszą umożliwiać skanowanie ruchu w warstwie aplikacji:   1. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie, 2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur, 3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem I łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur. |
|  | System IPS/Antywirus nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików. |
|  | Skanowanie IPS/Antywirus musi być możliwe między strefami bezpieczeństwa. |
|  | Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi. |
|  | Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p. |
|  | Wymagane jest dostarczenie dodatkowego urządzenia pełniące funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka. |
|  | Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji oraz zapewnienie wsparcia technicznego 24x7 na okres 36 miesięcy.. |
|  | Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i generowania na ich podstawie raportów. W celach zapewnienia kompatybilności oprogramowanie powinno pochodzić od tego samego producenta co system firewall. Wymagana jest licencja, która pozwoli na korzystanie z oprogramowania przez okres 36 miesięcy. |

# Duplikator z komputerem sterującym i monitorem

### Duplikator – 1 sztuka

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Szybkość publikowania (nagrywanie i drukowanie)** | min. 30 nośników CD-R / na godzinę. |
| min. 15 nośników DVD / na godzinę. |
| **Liczba pojemników wejściowych** | 2 |
| **Liczba pojemników wyjściowych** | 1 |
| **Pojemność pojemników wejściowych** | 100 |
| **Pojemność pojemnika wyjściowego** | 50 |
| **Rozdzielczość drukowania** | 1440 x 1440 dpi. |
| **Liczba pojemników z tuszem** | 6 |
| **Liczba napędów CD** | 2 |
| **Waga** | nie więcej niż 25 kg. |
| **Zużycie energii** | średnie nie więcej niż 86 W. |
| **Komunikacja** | Interfejs Gigabit Ethernet. |
| **Gwarancja** | 36 miesięcy. |

### Komputer do duplikatora – 1 sztuka

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **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 musi osiągać w teście wydajności PassMark PerformanceTest (wynik według stanu na stronie https://www.cpubenchmark.net/cpu\_list.php) co najmniej wynik 8900 punktów Passmark CPU Mark. |
| **Pamięć operacyjna RAM** | 8GB typu DDR4 2933 MHz możliwość rozbudowy do min. 32 GB. |
| **Parametry pamięci masowej** | Min. 256 GB NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. |
| **Grafika** | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla DirectX 12, OpenGL 4.5 |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, port do podłączenia zestawu słuchawkowego z przodu obudowy |
| **Obudowa** | 1. Typu mini-PC wyposażona w min. co najmniej jedną kieszeń wewnętrzną. 2. Zewnętrzny zasilacz o mocy maksimum 65 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności 88. 3. Musi istnieć możliwość zasilania komputera za pomocą portu USB-C. 4. W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. 5. Komputer powinien być wyposażony w zabezpieczenie umożliwiające zablokowanie dostępu do wnętrza komputera za pomocą linki Kensignton w taki sposób by bez odpięcia linki nie było możliwości otwarcia obudowy. 6. Możliwości montażu do tyłu monitora za pomocą dedykowanego uchwytu stanowiącego fabryczne rozwiązanie producenta komputera. 7. Uchwyt do montażu komputera do złącza VESA w monitorze. |
| **Zgodność z systemami operacyjnymi** | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi. |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane w procesorze. |
| **BIOS** | 1. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: 2. wersji BIOS, 3. ilości i sposobu obłożenia slotów pamięciami RAM, 4. typie procesora wraz z informacją o taktowaniu, 5. producencie, modelu i pojemności zainstalowanego dysku, 6. MAC adresie zintegrowanej karty sieciowej, 7. Prędkości obrotowej wentylatora chłodzącego procesor, 8. Temperaturze procesora, pamięci, dysku M.2 oraz chipsetu. 9. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS). 10. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. 11. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego . 12. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. 13. Możliwość włączenia/wyłączenia modułu TPM wraz z informacją o rodzaju modułu. 14. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów oraz możliwość wyłączenia wszystkich portów oprócz tych do których podłączone są klawiatura i mysz. 15. Możliwość ustawienia bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.: 16. liczby aktywnych rdzeni procesora, 17. trybu pracy karty sieciowej, 18. możliwości aktualizacji BIOS-u w tym co najmniej: całkowite wyłączenie możliwości aktualizacji, możliwość aktualizacji za pomocą narzędzi producenta komputera lub mechanizmu Windows Update, możliwość aktualizacji jedynie za pomocą narzędzi producenta komputera. |
| **Dodatkowe oprogramowanie** | 1. Umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu. 2. Certyfikowane oprogramowanie umożliwiające w bezpieczny (bezpowrotny) sposób usunięcie danych metodą 7 oraz 35 przebiegową z dysku twardego z poziomu BIOS-u bez względu na stan czy obecność systemu operacyjnego. 3. System diagnostyczny dostępny z poziomu BIOS oraz menu bootowania umożliwiający przetestowanie podzespołów komputera w tym co najmniej procesora, pamięci oraz dysku. |
| **Ergonomia** | 1. Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 17 dB. 2. Moduł konstrukcji obudowy w jednostce centralnej komputera (po odkręceniu dwóch śrub mocujących) powinien pozwalać na demontaż pamięci RAM, karty WLAN i dysku 2,5 cala bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). 3. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej. 4. Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 35 cm. |
| **Certyfikaty i standardy** | 1. Komputery mają spełniać normy i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie: 2. Deklaracja zgodności CE, 3. Wymagany wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - dopuszcza się wydruk ze strony internetowej, 4. Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001. 5. Potwierdzenie, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca posiadał Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi -odpowiadającej normie ISO 9001- (załączyć dokument potwierdzający spełnianie wymogu). 6. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram |
| **Wymagania dodatkowe** | 1. Wbudowane porty minimalnie: 2. 1 x HDMI, 3. 1 x Display Port, 4. 1 x RJ-45, 5. 1 x Audio: typu combo line-in/mikrofon ( z przodu), 6. 1 x USB 3.0 z przodu obudowy, 7. 1 x USB-C z przodu obudowy, 8. 2 x USB 2.0 z tyłu obudowy, 9. 1 x USB-C z tyłu obudowy z funkcją DP 1.4, 10. 2 x USB 3.2 z tyłu obudowy, 11. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. 12. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika). 13. Zintegrowany z płytą główną 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 (TPM co najmniej w wersji 2.0). 14. Minimum 2 złącza SO DIMM z obsługą do 32 GB DDR4 pamięci RAM, min. 1 złącza SATA III (6 Gbit), minimum 2 złącza M.2 w tym co najmniej jedno typu M.2-2280 (typu PCIe 3.0 x4 i przepustowości do 32 Gbit/s) umożliwiające instalację dysku SSD PCIe NVMe. 15. Klawiatura USB w układzie QWERTY US. 16. Mysz optyczna USB z trzema klawiszami oraz rolką (scroll) min 800dpi. |
| **Warunki gwarancji producenta** | 1. Na okres co najmniej 24 miesiące - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. 2. Czas reakcji na zgłoszoną reklamację gwarancyjną polegający na wizycie serwisanta w miejscu użytkowania- do końca następnego dnia roboczego. 3. Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| **Wsparcie techniczne producenta** | 1. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. 2. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera. |
| **System operacyjny** | Zainstalowany system operacyjny Windows 10 Professional lub równoważny.  *Opis równoważności*  Zainstalowany system operacyjny spełniający poniższe wymagania:   1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. 2. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW. 3. Internetowa aktualizacja zapewniona w języku polskim. 4. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 6. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). 7. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 8. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 9. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 10. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 11. 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. 12. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 13. Wbudowany system pomocy w języku polskim. 14. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 15. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 17. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.50. 18. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 19. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 20. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 21. Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. 22. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 23. 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. 24. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 25. Graficzne środowisko instalacji i konfiguracji. 26. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 27. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 28. Udostępnianie modemu. 29. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 30. Możliwość przywracania plików systemowych. 31. 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.). 32. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 33. Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit. 34. Licencja i oprogramowanie musi być nowe, nieużywane. |

### Monitor – 1 sztuka

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Ekran** | 23,8 cala o rozdzielczości natywnej minimum 1920x1080 pikseli, maksymalny rozmiar piksela 0.275 mm, matryca matowa, pokryta powłoką 3H, technologia matrycy IPS. |
| **Parametry obrazu** | Odwzorowanie 16.7 miliona kolorów, kontrast typowy 1000:1,  jasność min. 250 cd/m2, czas reakcji matrycy max. 5ms, kąty widzenia pionowe/poziome minimum 178/178 stopni. |
| **Wejścia wideo i inne** | 1x DP, 1x DVI-D, 1x D-SUB, wejście/wyjście audio. |
| **Obudowa i  regulacja monitora** | Pochylenie ekranu w zakresie -5° / +22°(tzw. Tilt), zintegrowany zasilacz i głośniki stereo o mocy minimum 2W każdy, możliwość regulacji głośności z menu OSD monitora, złącze Kensington Lock, złącze montażu na ścianie w standardzie VESA. |
| **Funkcje zarządzana energią i parametrami wyświetlania obrazu** | Technologia zapewniająca  zużycie energii przez monitor w trybie power save na poziomie 0.2W pozwalająca na redukcję ogólnego zużycia energii przez monitor (bez konieczności manualnego wyłączania monitora przez użytkownika), zgodność z normą Energy Star 8.0, zużycie energii przy ustawieniach EPA max. 14W. |
| **Menu monitora** | 1. Regulacja głośności. 2. Regulacja jasności. 3. Regulacja kontrastu. 4. Regulacja koloru (sRGB, 5000K, 6500K, 7500K, Użytkownika (R,G,B). 5. Menu w języku polskim oraz angielskim. |
| **Kable** | Kabel DVI-D o długości minimum 1.8m, kabel zasilający o długości minimum 1,8m, kabel audio. |
| **Gwarancja** | 1. Gwarancja 24 miesiące, wymiana lub naprawa monitora w miejscu użytkowania, następnego dnia roboczego od zgłoszenia. 2. Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| **Certyfikaty i normy, dokumentacja** | 1. Klasa energetyczna A+. 2. TCO 8.0. 3. Epeat bronze. 4. TÜV Low Blue Light Certified. 5. TÜV Flicker Free Certified. 6. CE. 7. ISO9241-307(klasa I). 8. RoHS, WEEE. 9. Instrukcja obsługi monitora. |

# Stacja RTG - 1 komplet

|  |  |
| --- | --- |
| **L.p.** | **Wymagane minimalne parametry techniczne** |
|  | Obudowa typu Tower. |
|  | Procesor min. 4-rdzeniowy 8-wątkowy, min 3.0GHz, osiągający w teście PassMark CPU Mark wynik min. 10000 punktów z wbudowanym kontrolerem pamięci DDR4 2400MHz z kontrolą parzystości ECC. |
|  | Pamięć RAM DDR4 2x4GB 2400 MHz ECC niebuforowane możliwość rozbudowy do min 64GB, minimum dwa sloty wolne na dalszą rozbudowę. |
|  | Karta graficzna zintegrowana z procesorem. |
|  | Dysk twardy:   1. Min. 2x500GB, 2. Konfiguracja dysków - RAID 1. |
|  | Zintegrowana z płytą główną karta sieciowa 1Gb Ethernet. |
|  | 1. System operacyjny Windows 10 Professional 64bit PL lub równoważny. 2. Opis równoważności przy „Komputerze dla duplikatora”. |
|  | Zasilacz 300W o sprawności minimum 90%. |
|  | Dedykowana przez producenta monitorów karta medyczna o następujących wymaganiach:   1. PCI Express x 16 Gen 3.0, 2. Pamięć DDR5 2GB, 3. 3 wyjścia cyfrowe mini DisplayPort, 4. Możliwość podłączenia do 4 monitorów jednocześnie, Sterowniki do systemów operacyjnych Windows 7(32/64 bit) Windows 8.1 (32/64 bit), Windows 10 (32/64 bit), 5. Pobór mocy do 30W, 6. Karta nisko-profilowa (Low Profile) . |
|  | 2 sztuki:  Medyczny LCD monitor monochromatyczny min. 21” o rozdzielczości 1600x1200, jasność maksymalna min. 1200 cd/m2, jasność skalibrowana min 500cd/m2, kontrast 1400:1, kalibracja sprzętowa DICOM. Licznik rzeczywistego czasu pracy monitora w OSD. LUT 13-bitowy, Matryca 10-bitowa, certyfikat Medical Device Class I, |
|  | 4 tryby pracy: standard DICOM, tryb kalibracji oddzielny dla złącza DVI i DP, tryb hybrydowy dla obrazów DICOM i innych wyświetlanych jednocześnie. |
|  | Wymagana sprzętowa kalibracja do standardu DICOM część 14 dla każdego trybu pracy. |
|  | Wbudowany kalibrator nie ograniczający pola widzenia na monitorze. |
|  | Funkcjonalność pozwalająca na samodzielne kalibrowanie monitora oraz sprawdzenie odcieni szarości bez systemu operacyjnego, uruchamiana z menu monitora. |
|  | Wymagany układ kontroli rzeczywistego czasu pracy monitora i jego podświetlenia. |
|  | Wymagane złącza: 1x DVI-D, 1x DisplayPort, 1x USB upstream, 2 x USB downstream |
|  | Przycisk za pomocą którego możemy w prosty sposób zmieniać tryby pracy monitora dla różnego rodzaju badań np. CT, CR. |
|  | Czujnik sprawdzający obecność użytkownika przed monitorem i pozwalający na jego automatyczne wyłączenie po odejściu użytkownika. |
|  | Czujnik mierzący jasność otoczenia. |
|  | Wymagany układ wyrównujący jasność i odcienie szarości dla całej powierzchni matrycy LCD z podświetleniem LED. |
|  | Komplet kabli zasilających i połączeniowych. |
|  | Automatyczne wyłączanie/włączanie monitora zsynchronizowane z wygaszaczem ekranu – po zainstalowaniu dołączonej do monitora aplikacji. |
|  | Możliwość zintegrowania z obudową monitorów diagnostycznych opcjonalnego oświetlenia obszaru za monitorem, z dodatkowym punktowym oświetleniem przestrzeni roboczej przed monitorem na elastycznym ramieniu, z możliwością regulacji poziomu jasności i opcją selektywnego wyłączenia obu podświetleń. |
|  | Monitor LCD min.22” tego samego producenta co monitor diagnostyczny, licznik rzeczywistego czasu pracy, rozdzielczość 1680x1050, wielkość piksela 0,282 mm, jasność 250cd/m2, kontrast  1000:1. |
|  | Urządzenie ochrony zasilania z wbudowaną ochroną przeciwprzepięciową  zgodną z normą IEC 61643-1 oraz spełniający normy IEC 62040-1, IEC 60950-1, IEC 62040-2, Raport CB, znak CE1  w płaskiej obudowie z możliwością pracy w pozycji pionowej i poziomej, wraz z oprogramowaniem umożliwiającym automatyczne wyłączenie systemu (uwzględniające zamknięcie badania) w przypadku braku zasilania. |
|  | Urządzenie musi posiadać minimum 4 gniazda FR z podtrzymaniem bateryjnym (odpowiednio 6 i 11 minut dla obciążenia 70% i 50%) i 4 gniazda FR z zabezpieczeniem przeciwudarowym (spełniający normę IEC 61643-1). |
|  | Funkcja odłączania urządzeń peryferyjnych w czasie czuwania. Możliwość montażu naściennego lub w szafie montażowej przy zastosowaniu dodatkowego zestawu montażowego. |
|  | Gwarancja:   1. Komputer – 24 miesiące, 2. Monitory diagnostyczne – 36 miesięcy. |
|  | Firma serwisująca monitory medyczne musi posiadać ISO 13485 na świadczenie usług serwisowych. |

# Rozmieszczenie sprzętu

### Serwer aplikacyjny – szt. 2

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

### Serwer bazodanowy – szt. 2

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

### Serwer domenowy – szt. 2

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

### Macierz dyskowa – szt. 1

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |

### UPS – szt. 2

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

### Przełącznik CORE – szt. 2

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

*Zamawiający dopuszcza inne rozmieszczenie Przełączników CORE, po przedstawieniu przez Wykonawcę projektu podłączenia sieci, po akceptacji Zamawiającego.*

### Switch dostępowy 48 – szt. 3

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu |
| 1 | 2 piętro szpitala – punkt dystrybucyjny - sekretariat oddziału terapii uzależnienia od alkoholu |
| 1 | Serwerownia zapasowa w budynku administracji – szafa PPD |

### Switch dostępowy 24 – szt. 5

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Poradnia Specjalistyczna Lidzbark Warmiński - rejestracja |
| 1 | Niski parter szpitala – punkt dystrybucyjny - korytarz |
| 1 | Wysoki parter szpitala – punkt dystrybucyjny - pokój socjalny |
| 1 | 1 piętro szpitala – punkt dystrybucyjny - brudownik |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

### Switch dostępowy 8 – szt. 3

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Ratownictwo medyczne Lidzbark Warmiński |
| 1 | Ratownictwo medyczne Orneta |
| 1 | Przychodnia Orneta – poradnia chirurgiczna |

### Przełącznik dostępowy PoE – szt. 3

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Wysoki parter szpitala – punkt dystrybucyjny – pokój socjalny |
| 1 | 1 piętro szpitala – punkt dystrybucyjny - brudownik |
| 1 | 2 piętro szpitala – punkt dystrybucyjny – sekretariat oddziału terapii uzależnienia od alkoholu |

### Switch dla potrzeb serwerów – szt. 2

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |
| 1 | Serwerownia zapasowa w budynku administracji – szafa |

*Zamawiający dopuszcza inne rozmieszczenie Switchów dla potrzeb serwerów, po przedstawieniu przez Wykonawcę projektu podłączenia sieci, po akceptacji Zamawiającego.*

### Access Point (AP) – szt. 38

|  |  |  |
| --- | --- | --- |
| **Nazwa oddziału** | **Liczba** | **Miejsca instalacji** |
| Oddział terapii uzależnienia od alkoholu | 1 | Sala chorych Nr 1 |
| Oddział terapii uzależnienia od alkoholu | 1 | Sala chorych Nr 2 |
| Oddział terapii uzależnienia od alkoholu | 1 | Sala chorych Nr 3 |
| Oddział terapii uzależnienia od alkoholu | 1 | Sala chorych Nr 4 |
| Oddział terapii uzależnienia od alkoholu | 1 | Sala chorych Nr 5 |
| Oddział terapii uzależnienia od alkoholu | 1 | Świetlica |
| Oddział terapii uzależnienia od alkoholu | 1 | Sala wykładowa |
| Oddział chirurgiczny | 1 | Sala chorych Nr 1 |
| Oddział chirurgiczny | 1 | Sala chorych Nr 2 |
| Oddział chirurgiczny | 1 | Sala chorych Nr 3 |
| Oddział chirurgiczny | 1 | Sala chorych Nr 4 |
| Oddział chirurgiczny | 1 | Sala chorych Nr 5 |
| Oddział chirurgiczny | 1 | Sala chorych Nr 6 |
| Oddział chirurgiczny | 1 | Sala chorych Nr 7 |
| Oddział chirurgiczny | 1 | Sala chorych pooperacyjna |
| Oddział pediatryczny | 1 | Sala chorych Nr 1 |
| Oddział pediatryczny | 1 | Sala chorych Nr 2 |
| Oddział pediatryczny | 1 | Separatka |
| Oddział pediatryczny | 1 | Sala chorych Nr 4 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 2 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 3 |
| Oddział wewnętrzny | 1 | Sala intensywnego nadzoru |
| Oddział wewnętrzny | 1 | Sala chorych Nr 5 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 6 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 7 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 8 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 9 |
| Oddział wewnętrzny | 1 | Sala chorych Nr 10 |
| Oddział chirurgii urazowo – ortopedycznej | 1 | Sala chorych Nr 1 |
| Oddział chirurgii urazowo – ortopedycznej | 1 | Sala chorych Nr 2 |
| Oddział chirurgii urazowo – ortopedycznej | 1 | Sala chorych Nr 3 |
| Oddział chirurgii urazowo – ortopedycznej | 1 | Sala chorych Nr 4 |
| Oddział ginekologiczny | 1 | Sala chorych Nr 1 |
| Oddział ginekologiczny | 1 | Sala chorych Nr 2 |
| Oddział ginekologiczny | 1 | Sala chorych Nr 3 |
| Oddział ginekologiczny | 1 | Sala obserwacyjna |
| Izba Przyjęć | 1 | Punkt pielęgniarski |
| Nocna i Świąteczna (POZ) | 1 | Gabinet lekarski |

### Kontroler AP – szt. 1

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |

### Firewall /UTM – szt. 1

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Serwerownia główna w szpitalu – szafa - Niski parter szpitala – część „A” |

### Duplikator z komputerem sterującym i monitorem – szt. 1

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Stanowisko personelu RTG - niski parter szpitala – część „B” |

### Stacja RTG – szt. 1

|  |  |
| --- | --- |
| **Liczba**  **sztuk** | **Miejsca instalacji** |
| 1 | Stanowisko opisowe lekarza RTG - niski parter szpitala – część „B” |

# Oprogramowanie systemowe

# Oprogramowanie do backupu – 1 sztuka

|  |  |
| --- | --- |
| **L.p.** | **Wymagane minimalne parametry techniczne** |
|  | Licencja z suportem na 36 miesięcy. Infrastruktura będzie wykorzystywała wirtualizację (2 serwery aplikacyjne z 4 CPU), reszta dotyczy maszyn fizycznych 4 sztuki – serwery bazodanowe i AD. |
|  | Oprogramowanie musi posiadać scentralizowaną administrację, jedna konsola zarządzająca. |
|  | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. |
|  | System backupowy powinien oferować dla serwerów produkcyjnych backup nie tylko po sieci LAN ale także po sieci SAN. |
|  | Oprogramowanie musi mieć możliwość monitowania i alterowania poprzez email. |
|  | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.7, 7.0 oraz Microsoft Hyper-V 2016 i 2019. |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V. |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
|  | Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. |
|  | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich. |
|  | System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. |
|  | System musi umożliwiać uruchomienie wirtualnej maszyny wprost z kopii zapasowej bez konieczności kopiowania wszystkich danych odtwarzanej maszyny wirtualnej do środowiska produkcyjnego. |
|  | Dopuszcza się zastosowanie oprogramowania agentowego dla serwerów fizycznych – bazodanowych i domenowych, umożliwiających granularne odzyskiwanie dla Active Directory, Microsoft Exchange, SQL Server, Sharepoint, Oracle. |
|  | Licencje musza być objęte 36-miesięcznym wsparciem producenta umożliwiającym dostęp do pomocy technicznej i do najnowszych wersji oprogramowania w trakcie trwania okresu wsparcia. |

# Systemy operacyjne serwerów

### Serwerowy system operacyjny dla potrzeb domeny – 2 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie** | Windows Server Standard Core 2019, licencja zgodna z oferowaną ilością corów CPU w serwerze domenowym z pkt. I.3 lub równoważne. |
| **Inne** | Wykonawca musi zapewnić dostęp do spersonalizowanej strony producenta produktów pozwalającej upoważnionym osobom ze strony Zamawiającego na:   1. pobieranie zakupionego oprogramowania, 2. pobieranie kluczy aktywacyjnych do zakupionego oprogramowania, 3. sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów. |
| **Sposób licencjonowania** | 1. Zamawiający nie dopuszcza licencji OEM. 2. Licencja musi mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. 3. Licencja musi umożliwiać downgrade do wcześniejszej wersji licencji (2016, 2012). |

*Serwerowy System Operacyjny – opis równoważności:*

|  |  |
| --- | --- |
| **L.p.** | **Wymagane minimalne parametry techniczne** |
|  | Licencja musi mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszta w przyszłym użytkowaniu. |
|  | Licencja obejmująca wszystkie rdzenie procesorów zainstalowanych w zaoferowanych serwerach wirtualnych. |
|  | Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty). |
|  | Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym lub dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. |
|  | **Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy:** |
|  | Możliwość wykorzystania min. 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym. |
|  | Możliwość wykorzystywania min. 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny. |
|  | Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych. |
|  | Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |
|  | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |
|  | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |
|  | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
|  | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. |
|  | Wbudowane wsparcie instalacji i pracy na wolumenach, które:   1. pozwalają na zmianę rozmiaru w czasie pracy systemu, 2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3. umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, 4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
|  | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |
|  | Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |
|  | Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET |
|  | Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. |
|  | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. |
|  | Graficzny interfejs użytkownika. |
|  | Zlokalizowane w języku polskim, następujące elementy:   1. menu, 2. przeglądarka internetowa, 3. pomoc, 4. komunikaty systemowe. |
|  | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
|  | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
|  | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
|  | Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). |
|  | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. 2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 3. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 4. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 5. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 6. Zdalna dystrybucja oprogramowania na stacje robocze. 7. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. 8. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 9. Dystrybucję certyfikatów poprzez http, 10. Konsolidację CA dla wielu lasów domeny. 11. Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen. 12. Szyfrowanie plików i folderów. 13. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 14. Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. 15. Serwis udostępniania stron WWW. 16. Wsparcie dla protokołu IP w wersji 6 (Ipv6). 17. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. 18. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: 19. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 20. Obsługi ramek typu jumbo frames dla maszyn wirtualnych, 21. Obsługi 4-KB sektorów dysków, 22. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 23. Możliwość kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model). 24. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
|  | Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
|  | Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). |
|  | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |
|  | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
|  | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
|  | Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

### Serwerowy system operacyjny dla potrzeb aplikacji oraz bazy danych – 4 sztuki

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie** | 1. Wykonawca dostarczy niezbędne oprogramowanie systemowe dla potrzeb systemu HIS. 2. Zamawiający dopuszcza rozwiązania open source. |

### Licencje dostępowe CAL – 150 sztuk

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie** | MS Windows 2019 DEV CAL lub równoważne. |
| **Sposób licencjonowania** | 1. Zamawiający nie dopuszcza licencji OEM. 2. Licencja musi mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. 3. Licencja musi umożliwiać downgrade do wcześniejszej wersji licencji (2012, 2008) oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń. |
| **Kompatybilność** | Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej. |

*Licencje dostępowe CAL – opis równoważności:*

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Sposób licencjonowania** | 1. Zamawiający nie dopuszcza licencji OEM. 2. Licencja musi mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. 3. Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. 4. Licencja musi umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń. |
| **Cechy** | Licencja musi zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla określonej liczby urządzeń. |
| **Kompatybilność** | Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej. |

# Oprogramowanie do wirtualizacji – 1 komplet

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie do wirtualizacji** | Licencja dla serwerów aplikacyjnych dwu procesorowych wraz z konsolą do zarządzania, ze wsparciem technicznym 9x5 oraz gwarancją utrzymania aktualnej wersji przez okres min. 36 miesięcy. |
| **Wymagania ogólne** | 1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. 6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 12. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami. 13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X. 14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 16. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. 17. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. 18. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 20. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 21. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. 22. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 23. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 24. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN). 25. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych. 26. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. 27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. 28. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. |

# Oprogramowanie do zarządzania domeną

### Licencje oprogramowania do zarządzania siecią – 1 komplet

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane minimalne parametry techniczne** |
| **Specyfikacja techniczna** | 1. Oprogramowanie musi posiadać budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program musi wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows. 2. Dane, które dotyczą działań pracownika na komputerze tj.: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Muszą być również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. 3. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administartorów. Działania administratorów muszą być logowane , co oznacza, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. |
| **Monitorowanie infrastruktury** | **MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO)** musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:   1. Wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping. 2. Wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU). 3. Wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci. 4. Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. 5. Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku. 6. Wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze. 7. Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie. 8. Wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny. 9. Zablokowania mapy urządzeń przed przypadkową edycją. 10. Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów. 11. Serwerów pocztowych: 12. program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, 13. program musi umożliwiać monitorowanie stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), 14. program musi umożliwiać wykonywania operacji testowych, 15. program musi umożliwiać wysłania powiadomienia jeśli serwer pocztowy nie działa. 16. Monitorowania serwerów WWW i adresów URL. 17. Cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS. 18. Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. 19. Obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID. 20. Obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych. 21. Monitoringu routerów i przełączników wg: 22. zmian stanu interfejsów sieciowych, 23. ruchu sieciowego, 24. podłączonych stacji roboczych – graficzna prezentacja panelu switcha, 25. ruchu generowanego przez podłączone do portów stacje robocze. 26. Serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie. 27. Wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu. 28. wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. 29. Program musi posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. 30. Program musi umożliwiać również definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy muszą być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 31. Program musi umożliwiać integrację ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP). |
| **Inwentaryzacja** | **W ZAKRESIE INWENTARYZACJI** program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:   1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne). 7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.   **Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:**   1. Przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji. 2. Tworzenie powiązań między zasobami a urządzeniami. 3. Tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych. 4. Wskazanie osób uprawnionych do użycia zasobów. 5. Definiowanie własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz. 6. Określenie atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów. 7. Określenie atrybutów dodatkowych tylko dla wybranych typów zasobów. 8. Definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie. 9. Import danych z zewnętrznego źródła (.CSV). 10. Przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp. 11. Tworzenie powiązań między zasobami a dokumentami w relacji 1:N. 12. Oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp. 13. Ewidencja czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności. 14. Generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania. 15. Generowanie protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji. 16. Archiwizacja i porównywanie audytów zasobów. 17. Tworzenie kodów kreskowych dla zasobów. 18. Drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy. 19. Inwentaryzacja zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android. 20. Inwentaryzacja stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline). 21. Definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”). |
| **Obsługa użytkowników** | **W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW** program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:   1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy). 2. Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. 3. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. 4. Informacji o edytowanych przez użytkownika dokumentach. 5. Historii pracy (cykliczne zrzuty ekranowe). 6. Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). 7. Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). 8. Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków. 9. Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.   **Program ponadto posiada możliwość:**   1. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. 2. Blokowania ruchu na wskazanych portach TCP/IP. 3. Blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem. 4. Wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia. 5. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 6. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. 7. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. 8. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. 9. Program musi posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych. |
| **Zdalna pomoc użytkownikom** | **PROGRAM MUSI UMOŻLIWIAĆ REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM.**   1. W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module musi znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie musi umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten musi zawierać komunikator (czat), który będzie umożliwiał przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). 2. Funkcjonalność modułu musi umożliwiać uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. 3. Moduł pomocy zdalnej musi umożliwiać: 4. pobieranie listy użytkowników z Active Directory, 5. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, 6. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, 7. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej, 8. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), 9. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 10. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 11. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 12. wykonywanie operacji na wielu zgłoszeniach równocześnie, 13. dołączanie załączników do zgłoszeń, 14. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 15. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 16. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 17. zrzuty ekranowe (podgląd pulpitu), 18. dystrybucję oprogramowania przez Agenty, 19. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 20. zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, 21. skonfigurowanie automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 22. planowanie nieobecności pracowników helpdesk, 23. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 24. generowanie raportów obsługi helpdesk, 25. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 26. zarządzanie procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 27. wymianę plików do i ze stacji roboczej poprzez funkcję Menedżera plików. |
| **Ochrona danych przed wyciekaniem** | **MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń:   1. Blokowanie urządzeń i nośników danych - program musi umożliwiać zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Blokownie musi dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 6. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 7. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane. 8. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 9. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 10. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. 11. Zarządzanie prawami dostępu do urządzeń - audyt operacji na plikach na urządzeniach przenośnych: 12. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych, 13. Podłączenie/odłączenie urządzenia przenośnego. 14. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 15. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. |
| **Ogólne** | 1. Ochrona przed usunięciem - program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. 2. Funkcjonalność Agenta - możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze. 3. Program dostępny jest w języku polskim, angielskim wraz z Podręcznikiem Użytkownika w formie strony internetowej. 4. Oprogramowanie musi umożliwiać zarządzanie 130 stacjami roboczymi z 60-miesięcznym wsparciem i możliwością aktualizacji. |