*Załącznik nr 2b do SIWZ*

**Szczegółowy opis przedmiotu zamówienia dla Zadania 2: Dostawa sprzętu komputerowego, w tym m.in. serwerów, macierzy, przełączników, stacji roboczych, urządzeń mobilnych i wielofunkcyjnych wraz z instalacją i konfiguracją** – dotyczy przetargu nieograniczonego na Informatyzację SPS ZOZ w Lęborku w ramach projektu „Wdrożenie interoperacyjnych i przygotowanych do integracji z platformą P1/P2 systemów informatycznych, w tym HIS/RIS/PACS w SPS ZOZ w Lęborku poprzez rozbudowę systemu obsługi informatycznej wszystkich procesów związanych z funkcjonowaniem szpitala zgodnie z zasadami określonymi w aktach prawnych dotyczących prowadzenia dokumentacji medycznej w wersji elektronicznej wraz z zakupem niezbędnego sprzętu komputerowego”

# Wymagania ogólne dla dostarczanych rozwiązań:

1. System powstały w wyniku niniejszego zamówienia musi funkcjonować zgodnie z obowiązującymi przepisami prawa w szczególności uwzględniać zmiany dotyczące przedmiotu realizacji projektu.
2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów.
3. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 9 miesięcy przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji poprawności działania.
4. Zamawiający zastrzega sobie prawo żądania przeprowadzenia testów poszczególnych funkcjonalności przed wyborem oferty.
5. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
6. Oferowane urządzenia w dniu składania oferty nie mogą być przeznaczone przez ich producenta do wycofania z produkcji lub sprzedaży.
7. Oferowane oprogramowanie w dniu składania oferty nie może być przeznaczone przez jego producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego.
8. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień poprzedzający dzień składania ofert.
9. Dla zaoferowanego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne oraz instrukcje obsługi.
10. Zamawiający wymaga, aby cały dostarczony sprzęt zarówno serwerowy jak i Kliencki (komputery, urządzenia peryferyjne) został skonfigurowany, uruchomiony i przetestowany przez Wykonawcę pod nadzorem pracowników Zamawiającego
11. Ilość zaplanowanego sprzętu serwerowego należy traktować jako minimalną. Wykonawca zobowiązany jest do dostarczenia odpowiedniej ilości sprzętu serwerowego, na którym będzie działał oferowany system HIS.
12. W przypadku wymiany systemu HIS/ERP na nowy, Wykonawca musi pozostawić istniejące macierze i serwery dla potrzeb istniejącego systemu HIS/ERP.
13. W ramach realizacji przedmiotu zamówienia w obszarze budowy środowiska serwerowo-macierzowego i dostawy sprzętu, Wykonawca zobowiązany będzie do realizacji poniższych zadań:
14. Przeprowadzić analizę przedwdrożeniowa i na jej podstawie opracować Projekt Wykonawczy wspólnie z Zamawiającym, który powinien obejmować:
	1. Wykaz dostarczanych urządzeń.
	2. Rysunki przedstawiające propozycje rozmieszczenia urządzeń w szafie serwerowej.
	3. Schemat sieci logicznej uwzględniający nowe urządzenia wraz z punktami styku sieci Zamawiającego.
	4. Opis wdrażanych rozwiązań
	5. Propozycję konfiguracji warstwy sieciowej.
	6. Propozycję konfiguracji serwerów i macierzy.
	7. Weryfikacja poprawności konfiguracji wdrażanej infrastruktury i określenie ewentualnych braków sprzętu/oprogramowania/licencje.

Projekt Wykonawczy musi zostać zaakceptowany przez Zamawiającego.

1. W ramach opracowywanego Projektu Wykonawczego szczegółowo opisać architekturę fizyczną wdrożenia systemu oraz jego konfigurację, zgodnie z którą przeprowadzone zostaną wdrożenia poszczególnych elementów Systemu.
2. Opracowania harmonogramu dostaw i konfiguracji elementów środowiska.
3. Dostawy wymaganego i opisanego poniżej sprzętu do lokalizacji Zamawiającego
4. Instalacji wskazanego sprzętu w szafie serwerowej RACK.
5. Uruchomienia i konfiguracji macierzy dyskowej na potrzeby wdrożenia systemu.
6. Uruchomienia i konfiguracji serwerów fizycznych na potrzeby serwera bazodanowego.
7. Uruchomienia i konfiguracji system ochrony danych (UTM).
8. Uruchomienia i konfiguracji systemu kopii zapasowych.
9. Instalacji dostarczonych urządzeń sieciowych oraz konfiguracji sieci LAN i WLAN, w tym podsieci VLAN zgodnie z wymaganiami opisanymi w Projekcie Wykonawczym.
10. Wdrożenia wirtualizacji oraz konfiguracji wysokiej dostępności dla potrzeb serwerów aplikacji, AD i wirtualizacji.
	1. Zidentyfikowane potrzeby Szpitala dotyczące maszyn wirtualnych:
		* ActiveDirectory1
		* ActiveDirectory2
		* FileServer
		* Serwer WSUS
		* Aplikacyjny1 - HIS
		* Aplikacyjny2 – ERP
		* Aplikacyjny3 – Lab
		* Aplikacyjny4 – Lab
		* GDATA
		* PlatformaIntegracyjna
		* ServerBackupu
		* LABO-WEB
		* MedycynaPracy
		* MPI-e-pacjent
		* E-uslugi
		* RCP
		* RUM
		* Testowy1
		* Testowy2
	2. Obecne serwery zostaną zwirtualizowane i uruchomione na nowym środowisku, ze względu na stan i jakość obecnych serwerów fizycznych. Obecny serwer bazodanowy musi pozostać na maszynie fizycznej (zaplanowano, że będzie on backupowany w całości przy pomocy dostarczanego oprogramowania do backupu).
11. Uruchomienia środowiska produkcyjnego i środowiska testowo-szkoleniowego Systemu.
12. Opracowania dokumentacji powykonawczej.

# Warunki gwarancji

1. Zamawiający wymaga minimum 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu komputerowego, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.
2. Zgłaszanie awarii musi następować w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta zaoferowanego sprzętu komputerowego.
3. W przypadku awarii dyski twarde pozostają u Zamawiającego.
4. Zamawiający wymaga dodatkowo wymaga:
5. dla kwalifikowanych podpisów elektronicznych i czytników do podpisów elektronicznych naprawy w ciągu 24h od daty i godziny zgłoszenia występowania usterki,
6. przez okres trwania gwarancji tzw. supportu dla motoru baz danych,
7. przez okres gwarancji upgrade oprogramowania do najnowszych wersji przez trzy lata, wraz ze wsparciem producenta dla Systemu zarządzania infrastrukturą IT.

Spis treści

[1. Sprzęt 5](#_Toc518325054)

[1.1. Serwer wirtualizacyjny – S1, S2 5](#_Toc518325055)

[1.2. Serwer backupowy / wirtualizacyjny – S3 7](#_Toc518325056)

[1.3. Serwer bazodanowy – S4, S5 9](#_Toc518325057)

[1.4. Macierz dyskowa 11](#_Toc518325058)

[1.5. Przełączniki serwerowe 13](#_Toc518325059)

[1.6. Zasilanie gwarantowane – UPS: 13](#_Toc518325060)

[1.7. Konsola KVM + KMM 16](#_Toc518325061)

[1.8. UTM Centrala 16](#_Toc518325062)

[1.9. Urządzenia mobilne 20](#_Toc518325063)

[1.10. Urządzenia wielofunkcyjne 26](#_Toc518325064)

[1.11. Skaner 28](#_Toc518325066)

[1.12. Kwalifikowane podpisy elektroniczne z czytnikiem 29](#_Toc518325067)

[1.13. Czytniki dokumentów tożsamości 29](#_Toc518325068)

[2. Oprogramowanie 31](#_Toc518325069)

[2.1 Wirtualizacja – systemy operacyjne – SSO1 31](#_Toc518325070)

[2.2 Systemy operacyjne dla serwerów bazodanowych – SSO2 BBB 33](#_Toc518325071)

[2.3. Licencje dostępowe dla SSO 36](#_Toc518325072)

[2.4 Motor bazy danych 37](#_Toc518325073)

[2.5 Oprogramowanie biurowe 38](#_Toc518325074)

[2.6 Oprogramowanie antywirusowe 41](#_Toc518325075)

[3. Systemy backupu i archiwizacji 46](#_Toc518325076)

[3.1. Biblioteka taśmowa 46](#_Toc518325077)

[3.2. Oprogramowanie do backupu 46](#_Toc518325078)

[4. Systemy bezpieczeństwa 48](#_Toc518325079)

[4.1. Wdrożenie AD 48](#_Toc518325080)

[4.2. System zarządzania infrastrukturą IT 48](#_Toc518325081)

[5. Szkolenia 63](#_Toc518325082)

[5.1. Szkolenie informatyczne (infrastruktura IT) 63](#_Toc518325083)

# Sprzęt

## Serwer wirtualizacyjny – S1, S2

|  |
| --- |
| **SERWER – 2 SZTUKI** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa** | Obudowa typu Rack o wysokości maksymalnej 2U, z możliwością instalacji do 8 dysków 3.5” HotPlug wraz z organizatorem kabli i kompletem szyn umożliwiających montaż w standardowej szafie Rack i bezpieczne wysuwanie serwera do celów serwisowych. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów.  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | 1. Zainstalowany jeden procesor dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku minimum 154 punkty w teście SPECrate2017\_int\_base dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej.
2. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora.
 |
| **RAM** | 128GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512GB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Mirror, Lockstep, Memory Rank Sparing |
| **Gniazda PCI** | Min. Trzy sloty PCIe Gen 3  |
| **Interfejsy sieciowe** | 1. Wbudowane 4 porty typu Gigabit Ethernet Base-T.
2. Zainstalowane dwie karty każda z 2 x 10Gb SFP+.
3. Wykonawca zobowiązany jest dostarczyć 4 sztuki kabli SFP+ to SFP+, 10GbE 3 Metry
 |
| **Dyski twarde** | 1. Możliwość instalacji dysków SATA, SAS, SSD.
2. Zainstalowane 2 dyski twarde SSD SATA o pojemności 240GB skonfigurowane w RAID1.
3. Możliwość instalacji wewnętrznego modułu dedykowany dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
 |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy. Możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. |
| **Wbudowane porty** | 1. 2 porty USB 2.0 (w tym 1-en port umożliwiający dostęp do karty zarządzającej)
2. 2 porty USB 3.0,
3. 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym),
4. 1 port RS232
 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |
| **Wentylatory** | Redundantne, Hot-Plug |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 750W. |
| **Bezpieczeństwo** | 1. Zintegrowany z płytą główną moduł TPM.
2. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
 |
| **Diagnostyka** | Panel LCD lub diody LED umieszczone na froncie obudowy lub panelu zabezpieczającym. |
| **Karta Zarządzania** | Karta zarządzania niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port RJ-45 Gigabit Ethernet i umożliwiająca:1. lokalną konfigurację poprzez wbudowane zarządzanie serwera,
2. wsparcie dla IPMI 2.0, SNMPv3,
3. możliwość uruchomienia zdalnego dostępu do graficznego interfejsu Web karty zarządzającej,
4. wbudowane narzędzia diagnostyczne,
5. umożliwiać lokalną instalację systemu operacyjnego  oraz aktualizacje oprogramowania wewnętrznego,
6. wsparcie dla protokołu Ipv6,
7. wsparcie dla remote CLI, oraz lokalnie dla CLI/SSH,
8. interfejs web musi wspierać 128 bit enkrypcję używając standardu SSL 3.0,
9. karta musi posiadać własny Web GUI, nie dopuszcza się potrzeby instalacji dodatkowego oprogramowania w celu korzystania z karty zarządzającej,
10. możliwość konfiguracji automatycznego wygaszania sesji (ilość sekund),
11. karta zarządzająca musi wysyłać powiadomienia/alarmy do administratora za pomocą SNMP oraz mailowo,
12. monitorowanie stanu serwera, możliwość sprawdzenia logów,
13. wirtualna konsola pozwalająca na zdalne podłączenie do serwera, możliwość połączenia także podczas restartu serwera. Możliwość konfiguracji BIOS z poziomu wirtualnej konsoli,
14. możliwość podpięcia wirtualnych napędów CD/DVD, FDD, ISO, klucz USB,
15. w zakresie bezpieczeństwa musi istnieć możliwość limitowania nieudanych prób logowania z konkretnego adresu IP, po przekroczeniu limitu dany adres musi być blokowany,
16. limitowanie zakresów adresów IP, z których można się podłączyć do karty zarządzającej,
17. możliwość rozszerzenia funkcjonalności o integracje z Active Directory, LDAP.
 |
| **Certyfikaty** | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
2. Serwer musi posiadać deklaracja CE.
3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Windows Server 2016.
 |
| **Dokumentacja użytkownika** | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
2. Sprawdzanie na stronie producenta przez podanie numeru fabrycznego konfiguracji sprzętowej serwera oraz warunków gwarancji.
3. Możliwość pobrania aktualnych sterowników ze strony internetowej producenta po podaniu numeru seryjnego serwera lub innego identyfikatora.
 |
| **Inne wymagania** | Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. |

## Serwer backupowy / wirtualizacyjny – S3

|  |
| --- |
| **SERWER - 1 SZTUKA** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa** | Obudowa typu Rack o wysokości maksymalnej 2U, z możliwością instalacji do 8 dysków 3.5” HotPlug wraz z organizatorem kabli i kompletem szyn umożliwiających montaż w standardowej szafie Rack i bezpieczne wysuwanie serwera do celów serwisowych. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów.  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | 1. Zainstalowany jeden procesor dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku minimum 154 punkty w teście SPECrate2017\_int\_base dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej.
2. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora.
 |
| **RAM** | 128GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512GB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Mirror, Lockstep, Memory Rank Sparing |
| **Gniazda PCI** | Min. Trzy sloty PCIe Gen 3  |
| **Interfejsy sieciowe** | 1. Wbudowane 4 porty typu Gigabit Ethernet Base-T.
2. Zainstalowane dwie karty każda z 2 x 10Gb SFP+.
3. Wykonawca zobowiązany jest dostarczyć 4 sztuki kabli SFP+ to SFP+, 10GbE 3 Metry
 |
| **Dyski twarde** | 1. Możliwość instalacji dysków SATA, SAS, SSD.
2. Zainstalowane 2 dyski twarde SSD SATA o pojemności 240GB skonfigurowane w RAID1.
3. Możliwość instalacji wewnętrznego modułu dedykowany dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
 |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy. Możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. |
| **Wbudowane porty** | 1. 2 porty USB 2.0 (w tym 1-en port umożliwiający dostęp do karty zarządzającej).
2. 2 porty USB 3.0.
3. 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym).
4. 1 port RS232.
 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |
| **Wentylatory** | Redundantne, Hot-Plug |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 750W. |
| **Bezpieczeństwo** | Zintegrowany z płytą główną moduł TPM.Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **Diagnostyka** | Panel LCD lub diody LED umieszczone na froncie obudowy lub panelu zabezpieczającym. |
| **Karta Zarządzania** | Karta zarządzania niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port RJ-45 Gigabit Ethernet i umożliwiająca:1. lokalną konfigurację poprzez wbudowane zarządzanie serwera,
2. wsparcie dla IPMI 2.0, SNMPv3,
3. możliwość uruchomienia zdalnego dostępu do graficznego interfejsu Web karty zarządzającej,
4. wbudowane narzędzia diagnostyczne,
5. umożliwiać lokalną instalację systemu operacyjnego  oraz aktualizacje oprogramowania wewnętrznego,
6. wsparcie dla protokołu Ipv6,
7. wsparcie dla remote CLI, oraz lokalnie dla CLI/SSH,
8. interfejs web musi wspierać 128 bit enkrypcję używając standardu SSL 3.0,
9. karta musi posiadać własny Web GUI, nie dopuszcza się potrzeby instalacji dodatkowego oprogramowania w celu korzystania z karty zarządzającej,
10. możliwość konfiguracji automatycznego wygaszania sesji (ilość sekund),
11. karta zarządzająca musi wysyłać powiadomienia/alarmy do administratora za pomocą SNMP oraz mailowo,
12. monitorowanie stanu serwera, możliwość sprawdzenia logów,
13. wirtualna konsola pozwalająca na zdalne podłączenie do serwera, możliwość połączenia także podczas restartu serwera. Możliwość konfiguracji BIOS z poziomu wirtualnej konsoli,
14. możliwość podpięcia wirtualnych napędów CD/DVD, FDD, ISO, klucz USB,
15. w zakresie bezpieczeństwa musi istnieć możliwość limitowania nieudanych prób logowania z konkretnego adresu IP, po przekroczeniu limitu dany adres musi być blokowany,
16. limitowanie zakresów adresów IP, z których można się podłączyć do karty zarządzającej,
17. możliwość rozszerzenia funkcjonalności o integracje z Active Directory, LDAP.
 |
| **Certyfikaty** | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
2. Serwer musi posiadać deklaracja CE.
3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Windows Server 2016.
 |
| **Dokumentacja użytkownika** | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
2. Sprawdzanie na stronie producenta przez podanie numeru fabrycznego konfiguracji sprzętowej serwera oraz warunków gwarancji.
3. Możliwość pobrania aktualnych sterowników ze strony internetowej producenta po podaniu numeru seryjnego serwera lub innego identyfikatora.
 |
| **Inne wymagania** | Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. |

## Serwer bazodanowy – S4, S5

|  |
| --- |
| **SERWER – 2 SZTUKI** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa** | Obudowa typu Rack o wysokości maksymalnej 2U, z możliwością instalacji do 8 dysków 3.5” HotPlug wraz z organizatorem kabli i kompletem szyn umożliwiających montaż w standardowej szafie Rack i bezpieczne wysuwanie serwera do celów serwisowych. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów.  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | 1. Zainstalowany jeden procesor dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku minimum 72 punkty w teście SPECrate2017\_int\_base dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej.
2. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora.
 |
| **RAM** | 128 GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512GB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Mirror, Lockstep, Memory Rank Sparing |
| **Gniazda PCI** | Min. Trzy sloty PCIe Gen 3  |
| **Interfejsy sieciowe** | 1. Wbudowane 4 porty typu Gigabit Ethernet Base-T.
2. Zainstalowane dwie karty każda z 2 x 10Gb SFP+.
3. Wykonawca zobowiązany jest dostarczyć 4 sztuki kabli SFP+ to SFP+, 10GbE 3 Metry
 |
| **Dyski twarde** | 1. Możliwość instalacji dysków SATA, SAS, SSD.
2. Zainstalowane 2 dyski twarde SSD SATA o pojemności 480GB skonfigurowane w RAID1.
3. Możliwość instalacji wewnętrznego modułu dedykowany dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
 |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy. Możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. |
| **Wbudowane porty** | 1. 2 porty USB 2.0 (w tym 1-en port umożliwiający dostęp do karty zarządzającej).
2. 2 porty USB 3.0.
3. 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym).
4. 1 port RS232.
 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |
| **Wentylatory** | Redundantne, Hot-Plug |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 750W. |
| **Bezpieczeństwo** | 1. Zintegrowany z płytą główną moduł TPM.
2. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
 |
| **Diagnostyka** | Panel LCD lub diody LED umieszczone na froncie obudowy lub panelu zabezpieczającym. |
| **Karta Zarządzania** | Karta zarządzania niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port RJ-45 Gigabit Ethernet i umożliwiająca:1. lokalną konfigurację poprzez wbudowane zarządzanie serwera,
2. wsparcie dla IPMI 2.0, SNMPv3,
3. możliwość uruchomienia zdalnego dostępu do graficznego interfejsu Web karty zarządzającej,
4. wbudowane narzędzia diagnostyczne,
5. umożliwiać lokalną instalację systemu ,operacyjnego  oraz aktualizacje oprogramowania wewnętrznego,
6. wsparcie dla protokołu Ipv6,
7. wsparcie dla remote CLI, oraz lokalnie dla CLI/SSH,
8. interfejs web musi wspierać 128 bit enkrypcję używając standardu SSL 3.0,
9. karta musi posiadać własny Web GUI, nie dopuszcza się potrzeby instalacji dodatkowego oprogramowania w celu korzystania z karty zarządzającej,
10. możliwość konfiguracji automatycznego wygaszania sesji (ilość sekund),
11. karta zarządzająca musi wysyłać powiadomienia/alarmy do administratora za pomocą SNMP oraz mailowo,
12. monitorowanie stanu serwera, możliwość sprawdzenia logów,
13. wirtualna konsola pozwalająca na zdalne podłączenie do serwera, możliwość połączenia także podczas restartu serwera. Możliwość konfiguracji BIOS z poziomu wirtualnej konsoli,
14. możliwość podpięcia wirtualnych napędów CD/DVD, FDD, ISO, klucz USB,
15. w zakresie bezpieczeństwa musi istnieć możliwość limitowania nieudanych prób logowania z konkretnego adresu IP, po przekroczeniu limitu dany adres musi być blokowany,
16. limitowanie zakresów adresów IP, z których można się podłączyć do karty zarządzającej,
17. możliwość rozszerzenia funkcjonalności o integracje z Active Directory, LDAP.
 |
| **Certyfikaty** | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
2. Serwer musi posiadać deklaracja CE.
3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Windows Server 2016.
 |
| **Dokumentacja użytkownika** | 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
2. Sprawdzanie na stronie producenta przez podanie numeru fabrycznego konfiguracji sprzętowej serwera oraz warunków gwarancji.
3. Możliwość pobrania aktualnych sterowników ze strony internetowej producenta po podaniu numeru seryjnego serwera lub innego identyfikatora.
 |
| **Inne wymagania** | Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. |

## Macierz dyskowa

|  |
| --- |
| **MACIERZ DYSKOWA – 1 KOMPLET** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Obudowa macierzy** | Do instalacji w standardowej szafie RACK 19”. Wysokość maksymalnie 2U wraz z kompletem szyn do montażu w szafie Rack z możliwością instalacji minimum 24 dysków 2.5” Hot Plug. |
| **Kontrolery** | 1. Dwa kontrolery posiadające łącznie minimum cztery porty iSCSI 10 Gb/s do podłączenia serwerów, pracujące w trybie active-active.
2. Wymagane poziomy zabezpieczenia RAID: 0,1,5,6,10.
 |
| **Dyski twarde w macierzy** | 1. Zainstalowane dyski w macierzy:
2. 5 dysków o pojemności minimum 960GB SSD SAS Hot-Plug 2.5” każdy,
3. 9 dysków o pojemności minimum 1,2TB SAS 10k Hot-Plug 2.5” każdy.
4. Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 190 dysków, wydajnych dysków SAS,SSD, ekonomicznych dysków typu NearLine SAS), samoszyfrujących dysków SED dostępnych w ofercie producenta macierzy, możliwość mieszania typów dysków w obrębie macierzy oraz półki.
 |
| **Oprogramowanie** | 1. Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków.
2. Funkcjonalność przestrzeni dyskowej typu cache, działających w ramach dedykowanych dysków SSD. Jeżeli funkcjonalność wymaga zakupu licencji, należy ją dostarczyć.
3. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 32 hostów bez konieczności zakupu dodatkowych licencji.
4. Zarządzanie macierzą poprzez minimum oprogramowanie zarządzające lub przeglądarkę internetową. Wymagana funkcja paska postępu – progress bar’u lub wyświetlenia wartości zaawansowania operacji w procentach przypadku formatowania wirtualnych dysków w oparciu o fizyczne dyski zainstalowane w macierzy.
5. Dodatkowe oprogramowanie umożliwiające wspólne zarządzanie oferowanymi serwerami oraz oferowaną macierzą poprzez sieć spełniające minimalne wymagania:
6. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych,
7. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta,
8. wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH,
9. możliwość oskryptowywania procesu wykrywania urządzeń,
10. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram,
11. szczegółowy opis wykrytych systemów oraz ich komponentów,
12. możliwość eksportu raportu do CSV, HTML, XLS,
13. grupowanie urządzeń w oparciu o kryteria użytkownika,
14. możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach,
15. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń,
16. szybki podgląd stanu środowiska,
17. podsumowanie stanu dla każdego urządzenia,
18. szczegółowy status urządzenia/elementu/komponentu,
19. generowanie alertów przy zmianie stanu urządzenia,
20. filtry raportów umożliwiające podgląd najważniejszych zdarzeń,
21. integracja z service desk producenta dostarczonej platformy sprzętowej ,
22. możliwość przejęcia zdalnego pulpitu,
23. możliwość podmontowania wirtualnego napędu,
24. automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu,
25. kreator umożliwiający dostosowanie akcji dla wybranych alertów,
26. możliwość importu plików MIB,
27. przesyłanie alertów „as-is” do innych konsol konsol firm trzecich,
28. możliwość definiowania ról administratorów,
29. możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów,
30. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania),
31. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta,
32. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów,
33. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
 |
| **Bezpieczeństwo** | 1. Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania.
2. Zasilacze, wentylatory, kontrolery RAID redundantne.
3. Możliwość przydzielenia większej przestrzeni dyskowej dla serwerów niż fizycznie dostępna (Thin Provisioning).
4. Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
 |
| **Dokumentacja** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |
| **Półka dyskowa** | 1. Dedykowana półka dyskowa przeznaczona do instalacji w standardowej szafie rack (maksymalnie 2U) umożliwiająca instalację 12 dysków 3,5”.
2. Zainstalowane 8 sztuk dysków 8TB NLSAS 7,2k Hot-Plug.
3. Zasilacze redundantne, hot-swap, moc maksymalna 600W.
4. Zainstalowane dwa moduły zarządzania obudową oraz 2 kable 1 metrowe SAS do podłączenia do macierzy dyskowej.
5. Zainstalowany moduł umożliwiający kaskadowe podłączanie kolejnych półek dyskowych.
 |
| **Certyfikaty** | 1. Macierz wyprodukowana zgodnie z normą ISO 9001 oraz 14001.
2. Zgodność z systemami operacyjnymi: Microsoft Windows, VMware, Microsoft Hyper-V, Citrix XenServer®, Red Hat oraz SUSE.
 |

## Przełączniki serwerowe

|  |
| --- |
| **PRZEŁĄCZNIKI SERWEROWE – 2 SZTUKI** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa** | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U. |
| **Porty** | 1. 20 portów 10 Gigabit Ethernet Base-T (wbudowane lub porty SFP+ obsadzone wkładkami 10 GbE Base-T),
2. 20 portów 10 Gigabit Ethernet SFP+ z 6 wkładami 10GbE SFP+ światłowodowymi (zgodnymi z oferowanym światłowodem).
 |
| **Rodzaj urządzenia** | Przełącznik warstwy L3 |
| **Przepustowość przełączania** | Min. 950 Gbit/s |
| **Przepustowość** | Min. 702 Mpps |
| **Pamięć RAM** | Min. 1 GB |
| **Pamięć flash** | Min. 256 MB |
| **MAC addresses** | 128 000 |
| **Inne** | 1. Obsługa ssl/ssh; pełny dupleks, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).
2. Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
 |

## Zasilanie gwarantowane – UPS:

|  |
| --- |
| **UPS dla potrzeb serwerów – 2 SZTUKI** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Technologia** | VFI (true on-line, podwójne przetwarzanie energii) |
| **Moc znamionowa** | 6 kVA / 6 kW |
| **Wyjściowy współczynnik mocy (PF)** | 1.0 |
| **Napięcie wejściowe**  | 230 Vac |
| **Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie** | 138– 299 Vac  |
| **Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie** | 110 – 299 Vac |
| **Częstotliwość wejściowa** | Wymagana 40-70 Hz |
| **Sprawność AC-AC w trybie pracy****on-line z obciążeniem 100%**  | nie mniejsza niż 95% |
| **Sprawność AC-AC w trybie pracy****Oszczędzania energii Eco Mode** | nie mniejsza niż 99% |
| **Tryb pracy z konwersją częstotliwości** | Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie. |
| **Napięcie wyjściowe**  | 230 Vac |
| **Częstotliwość wyjściowa** | 50/60Hz (programowalna) |
| **Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem** | Wymagane |
| **Czas podtrzymania** | 9 minut dla 100 % obciążenia. |
| **Baterie** | Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat i pojemności minimalnej 2 160 V\*Ah. |
| **Szafa baterii** | Zamknięta szafa bateryjna |
| **Stabilizacja napięcia wyjściowego w stanie ustalonym** | ± 1% |
| **Stabilizacja napięcia wyjściowego w stanie nieustalonym** | ± 3% |
| **Współczynnik szczytu** | 3:1 |
| **Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną** | Wymagane |
| **Złącze interfejsów** | RS232, USB, REPO. |
| **Karta sieciowa SNMP** | Wymagana |
| **Interfejs EPO (do wyłącznika ppoż.)** | Wymagane |
| **Diagnostyka parametrów urządzenia UPS i baterii** | Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS. |
| **Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego** | Wymagane |
| **Poziom hałasu w odległości 1m,** | 1. < 50 Dba
2. Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury.
 |
| **Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu** | Wymagane |
| **Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE** | Wymagane |
| **Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.** | Wymagane |
| **Certyfikat ISO 9001 oraz 14001 producenta zasilacza UPS** | Wymagane |
| **Wymiary zasilacza UPS w szafie rack 19’’** | Maks 5 U |
| **Szyny do montażu w szafie rack** | Wymagane |
| **Instrukcja w języku polskim** | Wymagane |
| **Podłączenie i uruchomienie do przygotowanej instalacji** | Autoryzowany serwis producenta oferowanego zasilacza UPS przeprowadzi instalację i uruchomienie urządzenia na obiekcie oraz przeprowadzi profesjonalne szkolenie z zakresu obsługi UPSa dla pracowników Zamawiającego. |
| **Uzgodnienia z Zamawiającym** | Wykonawca wykona przyłącze do oferowanego UPS-a zgodnie z zaleceniami producenta UPS-a oraz zgodnie z wytycznymi Zamawiającego.  |

## Konsola KVM + KMM

|  |
| --- |
| **KONSOLA KVM + KMM – 1 SZTUKA** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa**  | Max. 1U do montażu w szafie rack |
| **Złącza**  | 1. Porty KVM: 16.
2. Mysz zewnętrzna: USB.
3. LAN: RJ-45.
 |
| **Funkcjonalność**  | 1. Hot Pluggable - umożliwia podłączanie i odłączanie PC bez wyłączania przełącznika.
2. Auto Scan ułatwia wybór i monitorowanie komputerów.
3. Auto Scan - monitorowanie połączenia z komputerem.
4. Przełącznik musi posiadać emulację klawiatury i myszy PS/2 przy bootowaniu komputerów.
5. Nie wymaga oprogramowania - praca przez menu OSD i skróty klawiaturowe.
6. Dodatkowy port konsolowy do podłączenia dodatkowego zestawu monitora, myszki i klawiatury.
7. Dodatkowe porty USB do podłączenia myszki oraz urządzeń peryferyjnych.
8. Możliwość nadawania nazw poszczególnym komputerom.
9. Dwa poziomy dostępu chronione hasłami (admin + 4 userów) - oddzielne profile.
10. Możliwość zarządzania poprzez IP – zdalna konsola - Użytkownicy zdalni uzyskują dostęp do przełącznika przez Internet za pomocą przeglądarki internetowej używającej protokołu TCP / IP do zdalnego protokołu komunikacyjnego.
 |
| **Wyświetlacz** | 1. 17" LCD.
2. Obsługa rozdzielczości do 1280x1024 przy 75 Hz dla lokalnej konsoli, do 1920x1200 dla zdalnego połączenia.
 |
| **Urządzenia wskazujące** | Klawiatura i touchpad |
| **Wyposażenie**  | 1. 1 x przewód zasilający.
2. 1 x zestaw do montażu w szafie rack.
3. 8 x Przewód KVM.
 |

## 1.8. UTM Centrala

|  |
| --- |
| **UTM CENTRALA - 1 KOMPLET dwóch****urządzeń pracujących w klastrze HA** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Typ urządzenia** | 1. Zapora sieciowa typu Next Generation Firewall (NGFW).
2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.
 |
| **Specyfikacja fizyczna** | * + - 1. Dedykowane rozwiązanie sprzętowe.
			2. Obudowa 1U przeznaczona do montażu w szafie RACK 19” oraz posiadająca oprzyrządowanie niezbędne do zamocowania w takiej szafie.
			3. Ilość interfejsów:
1. 2 interfejsy 10 GbE SFP+,
2. 8 interfejsy 2.5 GbE SFP,
3. 4 interfejsy 2.5 GbE,
4. 12 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa,
5. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G,
6. 1 interfejs konsoli do zarządzania zaporą,
7. 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą.
	* + 1. Zapora powinna posiadać dysk SSD o pojemności przynajmniej 32 GB z możliwością wymiany na większy.
 |
| **Funkcjonalności** | 1. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa.
2. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji.
3. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q.
4. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP.
5. 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).
6. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa).
7. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP.
8. Wsparcie dla Dynamicznego DNS tzw. DDNS.
9. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
10. 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).
11. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
12. wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),
13. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,
14. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
15. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps.
16. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
17. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
18. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
19. 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).
20. Kontrola dostępności zestawionych tuneli VPN.
21. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
22. 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.
23. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić).
24. Funkcja NAT oparta o reguły bezpieczeństwa.
25. 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).
26. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
27. Zintegrowany system skanowania antyspyware.
28. 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.
29. System IPS musi używać algorytmu szeregowego przetwarzania.
30. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
31. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji:
32. bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie,
33. administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,
34. administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
35. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
36. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa.
37. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi.
38. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p.
39. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń.
40. Urządzenie powinno posiadać możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 3 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Licencja na tą funkcjonalność powinna być ważna przez okres 3 lat.
 |
| **Wydajność urządzenia** | 1. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej.
2. Minimalna ilość jednocześnie obsługiwanych połączeń: 2 000 000.
3. Możliwość obsłużenia przynajmniej 14 000 nowych połączeń w ciągu 1 sekundy.
4. Przepustowość urządzenia pracującego w trybie stateful firewall: 3,75 Gbps – dla ramki 1518B zgodnie z RFC 2544.
5. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.8 Gbps.
6. Przepustowość urządzenia pracującego jako koncentrator VPN: 1.5 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544.
7. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 730 Mbps.
8. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3 000.
9. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 500 z możliwością rozszerzenia do przynajmniej 3 000.
10. 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.
11. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 300 Mbps oraz obsłużyć 15 000 połączeń.
 |
| **Klaster** | 1. Wymagane jest dostarczenie dodatkowego urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym.
2. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka.
 |
| **Wymagane licencje** | 1. 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 3 lat.
2. 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 5 lat.
 |
| **Dodatkowe wyposażenie** | 2 sztuki wkładek 10 GbE SPF+ kompatybilnych z urządzeniem. |

## Urządzenia mobilne

|  |
| --- |
| **LAPTOPY 2 SZTUKI + 2 SZTUKI DLA PARTNERÓW** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Zastosowanie** | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| **Przekątna Ekranu** | Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED i powłoką przeciwodblaskową, jasność 220 nits, kontrast 400:1, maksymalny rozmiar plamki 0,180 mm. |
| **Procesor** | 1. Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 7000 punktów Passmark CPU Mark.
2. Wynik dostępny na stronie : <http://www.passmark.com/products/pt.htm>
 |
| **Płyta główna** | Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta i oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera.  |
| **Pamięć RAM** | **8GB** DDR4 2400MHzmożliwość rozbudowy do min 32GB, wymagane min. 2 sloty na pamięci w tym min. jeden wolny,pracująca z procesorem na magistrali 2400MHz |
| **Pamięć masowa** | 128GB SSD SATA M.2 2280 |
| **Karta graficzna** | Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej. Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 900 punktów w G3D Rating, wynik dostępny na stronie: <http://www.videocardbenchmark.net/gpu_list.php>  |
| **Klawiatura** | Klawiatura wyspowa w układzie QUERTY, powłoka antybakteryjna, z wbudowanym w klawiaturze podświetleniem, (układ US -QWERTY), min 100 klawiszy, z prawej strony wydzielona klawiatura numeryczna. |
| **Multimedia** | 1. Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki stereo o średniej mocy 2x 2W i szczytowej 2x 2,5W, wbudowany wewnętrzny wzmacniacz głośników.
2. Kamera internetowa z diodą informującą o aktywności, o rozdzielczości min. 1280x720, trwale zainstalowana w obudowie matrycy.
3. Czytnik kart SD, 1 port audio typu combo (słuchawki i mikrofon).
 |
| **Łączność bezprzewodowa** | Karta sieci bezprzewodowej WiFi 802.11ac z dwoma antenami + bluetooth min. 4.1. |
| **Bateria i zasilanie** | 1. Min. 56Whr Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.
2. Zasilacz o mocy max. 65W.
 |
| **Obudowa** | 1. Szkielet obudowy i zawiasy notebooka wykonany z wzmacnianego metalu, dookoła matrycy gumowe uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią.
2. Komputer spełniający normy MIL-STD-810G [załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta] z zakresu przeprowadzonych testów:
3. Method 500.5Procedure I,
4. Method 500.5Procedure II,
5. Method 501.5Procedure I,
6. Method 501.5Procedure II,
7. Method 502.5 Procedure I,
8. Method 502.5Procedure II,
9. Method 510.5Procedure I,
10. Method 514.6Procedure I Cat. 4,
11. Method 514.6Procedure I Cat. 24,
12. Method 516.6Procedure I,
13. Method 516.5Procedure II,
14. Method 516.6Procedure VI,
15. Method 516.5Procedure V.
 |
| **Środowisko pracy** | 1. Zakres temperatur pacy : od 0 do 50 °C.
2. Zakres przechowywania : od -40 do 65 °C.
3. Załączyć oświadczenie wykonawcy poparte oświadczeniem producenta.
 |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **BIOS** | 1. BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera, kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach.
2. Funkcje BIOS :
3. musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Dopuszcza się aby po wprowadzeniu hasła systemowego była możliwość jedynie zmiany hasła systemowego i hasła dla dysku twardego (jeśli zostało zdefiniowane), po podaniu hasła systemowego użytkownik nie może zmieniać ustawień ani konfiguracji daty i godziny,
4. możliwość włączenia/wyłączenia zintegrowanego kontrolera USB,
5. możliwość włączenia/wyłączenia dosilenia portu USB,
6. możliwość włączenia/wyłączenia zintegrowanego kontrolera audio,
7. możliwość włączenia/wyłączenia zintegrowanego mikrofonu,
8. możliwość włączenia/wyłączenia zintegrowanych głośników,
9. możliwość włączenia/wyłączenia szybkiego ładownia baterii,
10. możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN – opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN,
11. możliwość włączenia/wyłączenia zabezpieczenie wykrywające uszkodzenie zasilacza lub wykrycie podłączenia zasilacza o niewłaściwym min. napięciu,
12. możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne,
13. możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
 |
| **Certyfikaty** | 1. Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty).
2. Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty).
3. Deklaracja zgodności CE (załączyć do oferty).
4. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
5. Potwierdzenie kompatybilności komputera na stronie Windows Logo'd Products List na daną platformę systemową (wydruk ze strony).
6. EnergyStar 6.0 – załączyć do oferty certyfikat lub oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta.
7. Certyfikat TCO, wymagana certyfikacja na stronie: [http://tco.brightly.se/pls/nvp/!tco\_search](http://tco.brightly.se/pls/nvp/%21tco_search) – załączyć do oferty wydruk z strony.
 |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 19dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta. |
| **Diagnostyka** | 1. System diagnostyczny z graficznym interfejsem użytkownika zaimplementowany w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty  o funkcjonalności:
2. testy uruchamiane automatycznie lub w trybie interaktywnym,
3. możliwość powtórzenia testów,
4. podsumowanie testów z możliwością zapisywania wyników,
5. uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu.
6. Uruchamianie testów zdefiniowanych przez użytkownika.
7. Wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów.
8. Wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.
9. Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera. Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o natywnej rozdzielczości matrycy, numerze seryjnym, typie i pojemności dysku twardego, o żywotności baterii – informacja podana w %, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, typ pamięci wraz z taktowanie oraz SN i PN, wykaz temperatur dla baterii, CPU, pamięci, temperatury panującej wewnątrz.
 |
| **Bezpieczeństwo** | 1. Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.
2. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
3. Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy.
 |
| **System operacyjny** | 1. Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS.
2. Opis równoważności - zainstalowany system operacyjny spełniający poniższe wymagania:
3. pełna integracja z posiadanymi modułami systemu informatycznego Asseco InfoMedica,
4. możliwość zainstalowania i użytkowania posiadanego przez Zamawiającego oprogramowania Microsoft Office 2010,
5. możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek,
6. możliwość dokonywania uaktualnień sterowników urządzeń przez Internet,
7. 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,
8. internetowa aktualizacja zapewniona w języku polskim,
9. wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,
10. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
11. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi),
12. funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
13. 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,
14. możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu,
15. zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,
16. 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,
17. zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,
18. wbudowany system pomocy w języku polskim,
19. możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),
20. możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
21. wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
22. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
23. rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
24. system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,
25. 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,
26. wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń,
27. zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
28. 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,
29. rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
30. graficzne środowisko instalacji i konfiguracji,
31. transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
32. zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
33. udostępnianie modemu,
34. oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
35. możliwość przywracania plików systemowych,
36. 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.),
37. możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
38. Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit,
39. licencja i oprogramowanie musi być nowe, nieużywane.
 |
| **Dodatkowe oprogramowanie** | 1. Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające:
2. określenie preferencji aktualizacji,
3. ustawienie priorytetu aktualizacji,
4. użycia opcji planowania aktualizacji bieżących wersji sterowników.
5. Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:
6. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
7. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:
	1. poprawkach i usprawnieniach dotyczących aktualizacji,
	2. dacie wydania ostatniej aktualizacji,
	3. priorytecie aktualizacji,
	4. zgodność z systemami operacyjnymi,
	5. jakiego komponentu sprzętu dotyczy aktualizacja,
	6. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.
8. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne,
9. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga,
10. rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr),
11. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania),
12. dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml,
13. raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
 |
| **Porty i złącza** | Wbudowane porty i złącza : 1x VGA, 1x HDMI 1.4, 1x RJ-45, 1x USB 3.1 w tym jeden port z zasilaniem, 1x USB 2.0, 1x USB TYP-C, port zasilania. |

## 1.10. Urządzenia wielofunkcyjne

|  |
| --- |
| **URZĄDZENIA WIELOFUNKCYJNE - 5 SZTUK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Drukowanie** |
| **Szybkość drukowania** | 40 str./min |
| **Czas pierwszego wydruku** | 5 sekund |
| **Rozdzielczość** | 1200 x 1200 dpi |
| **Czcionki druku** | 87 skalowanych czcionek PCL |
| **Języki druku** | PCL5e, PCL6 |
| **Zespół drukowania** | Dupleks mechaniczny |
| **Skanowanie** |
| **Rozdzielczość skanowania**  | 600 x 600 dpi |
| **Szybkość skanowania**  | Do 6 s/stronę w kolorze i 2 s/stronę w trybie monochromatycznym |
| **Głębia kolorów**  | Wejście 48 bit/Wyjście 24 bit |
| **Podawanie dokumentów**  | Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski |
| **Format**  | M-TIFF, PDF, XPS, JPEG, GIF, PNG |
| **Książka adresowa**  | LDAP lub 300 adresów e-mail i 20 grup adresowych |
| **Skanowanie do**  | FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB |
| **Kopiowanie** |
| **Czas wykonania pierwszej kopii**  | 10 sekund |
| **Szybkość kopiowania**  | do 37 kopii/min |
| **Rozdzielczość kopiowania**  | do 600 x 600dpi |
| **Zmniejszanie/powiększanie**  | Zoom 25-400% |
| **Maksymalna liczba kopii** | 99 |
| **Faksowanie** |
| **Złącza** | RJ11 x 2 (Line/Tel), PSTN, Linia PBX |
| **Szybkość**  | ITU-T G3(Super G3) do 33,6kbps, do 2 s/str. |
| **Szybkie wybieranie**  | 40 numerów w wybieraniu jednodotykowym, 100 numerów szybkiego wybierania |
| **Lista rozgłaszania**  | Maksimum 100 |
| **Pamięć stron** | 4MB |
| **Interfejs i oprogramowanie** |
| **Złącza**  | Port USB 2.0, Ethernet 10/100/1000BaseTX |
| **Komunikacja bezprzewodowa** | Nie |
| **Kompatybilność z systemami operacyjnymi**  | Windows 7 (32-bit & 64-bit), Windows 8 (32-bit & 64-bit), Windows 8.1 (32-bit & 64-bit), Windows Server 2003 (32-bit & 64-bit), Windows Vista (32-bit & 64-bit), Windows Server 2008 (32-bit & 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (32 bit & 64 bit); Linux PPD; Mac OS 10.6.8 - 10.7, 10.8, 10.9 |
| **Dodatkowe oprogramowanie**  | 1. Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje:
2. funkcjonować w środowisku Windows,
3. obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT),
4. podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki,
5. podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku,
6. możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek,
7. podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów),
8. możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.
 |
| **Podawanie papieru** |
| **Pojemność papieru**  | 1. Podajnik 1: 250 arkuszy 80 g/m2.
2. Podajnik uniwersalny: 100 arkuszy 80 g/m2.
3. Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2.
 |
| **Format papieru**  | 1. Podajnik 1: A4, A5, B5, A6.
2. Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, nośniki (baner) do 130 cm długości.
3. Druk dwustronny: A4, B5, A5.
 |
| **Gramatura papieru**  | 1. Podajnik 1: 60 – 160 g/m2.
2. Druk dwustronny: 60 – 120 g/m2.
3. Podajnik uniwersalny: 60 – 160 g/m2.
4. Podajnik skanera: 60 – 105 g/m2.
 |
|  **Odbiornik papieru**  | Do 150 arkuszy stroną zadrukowaną do dołu |
| **Pozostałe parametry techniczne** |
|  **Pamięć**  | Standardowa pamięć RAM: 512 MB, 3 GB pamięci eMMC. |
|  **Szybkość procesora**  | 667 MHz |
|  **Obciążenie** | Maksymalne obciążenie do 80 000 stron miesięcznie. |
|  **Materiały eksploatacyjne:** | Wymagana rozdzielność bębna i tonera.  |

1.

## Skaner

|  |
| --- |
| **SKANER - 4 SZTUKI** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Typ skanera** | Skaner płaski |
| **Rozdzielczość skanowania** | 1200x1200 DPI |
| **Ultradźwiękowy czujnik** | Tak |
| **Źródło światła** | Technologia diodowa |
| **Prędkość skanowania** | 1. Monochromatyczny 25 Str./min.
2. Kolor: 25 Str./min.
 |
| **Podajnik ADF** | 1. Pojemność 50 Arkuszy.
2. Skanowanie dwustronne.
3. Rozdzielczość 600x600 DPI.
 |
| **Dzienna wydajność** | 1500 Stron |
| **Funkcje skanowania** | Automatyczna korekta położenia ukośnego, Poprawa tekstu, Rozszerzona edycja obrazu, Pomijanie pustych stron, Automatyczny obrót obrazu. |
| **Złącza** | USB 3.0 |

## Kwalifikowane podpisy elektroniczne z czytnikiem

|  |
| --- |
| **KWALIFIKOWANE PODPISY ELEKTRONICZNE Z CZYTNIKIEM I WAŻNOŚCIĄ** **PODISÓW na 3 LATA - 15 SZTUK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Ważność certyfikatów** | 36 miesięcy |
| **Czytnik kart** | USB |
| **Typ karty kryptograficznej** | SIM |
| **Obsługa** | Rejestracja podpisów w systemach szpitalnych. |
| **W Zestawie** | Karta kryptograficzna, czytnik USB, Płyta z oprogramowaniem. |

## Czytniki dokumentów tożsamości

|  |
| --- |
| **CZYTNIKI DOKUMENTÓW TOŻSAMOŚCI - 8 SZTUK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Zastosowanie** | Czytnik OCR pozwalające na szybką identyfikację danych zadrukowanych na kartach plastikowych jak i na dokumentach papierowych. |
| **Sensor CCD** | 24 bit/pixels-RGB, 8 bit/pixels (podczerwień) 450 DPI. |
| **Przechwytywanie obrazu** | W świetle białym i podczerwonym. |
| **Odczyt** | 1. Strefy MRZ z dowodu osobistego I paszportu strefy VIZ z dowodu osobistego, prawo jazdy oraz karty studenckiej.
2. Kodów kreskowych: 1D -UPC-A, EAN8, EAN13, Code39, Code128, Interleaved 2 of 5.
3. 2D – PDF 417, Data Matrix, QR Code, Aztec Code ICAO 9303.
 |
| **Budowa** | Brak części ruchomych. |
| **Okno skanowania** | 4 mm szkło hartowane |
| **Interfejs** | USB z odłączanym kablem komunikacyjnym |
| **Zasilanie** | Przez USB |
| **Sygnalizacja** | Wizualna – 3 programowalne diody LED |
| **Oprogramowanie** | 1. Program OCR – oprogramowanie do współpracy z czytnikami w zakresie rozpoznawania tekstów spoza zapisów MRZ na polskich dokumentach tożsamości: paszport, dowód osobisty, prawo jazdy. Dostępne są także odczyty z innych dokumentów.
2. Wymaga corocznej opłaty aktualizacyjnej – Wykonawca zapewni aktualizację na 5 lat.
 |

# Oprogramowanie

## 2.1 Wirtualizacja – systemy operacyjne – SSO1

|  |
| --- |
| **LICENCJA SSO1 - 3 SZTUKI** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie** | Microsoft 2016 Data Center 64bit z licencją obejmującą wszystkie cory procesora zainstalowanego w zaoferowanym serwerze wirtualizacyjnym: S1, S2, S3 – licencja na nie mniej niż 16 core - w licencjonowaniu dla jednostek rządowych lub równoważne |
| **Inne** | Wykonawca zapewni 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. Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
2. Zamawiający wymaga typu licencji MOLP (Microsoft Open License Program) w licencjonowaniu dla jednostek rządowych.
3. 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 i nielimitowaną liczbę wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
 |

***Serwerowy System Operacyjny (SSO1) – opis równoważności:***

|  |
| --- |
| ***Wymagane minimalne parametry techniczne***  |
| 1. Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszta w przyszłym użytkowaniu.
2. Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).
3. 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 i nielimitowaną liczbę wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
 |
| Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy. |
| 1. Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym
 |
| 1. Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
 |
| 1. Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
 |
| 1. Posiada 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.
 |
| 1. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 |
| 1. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 |
| 1. Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 |
| 1. Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 |
| 1. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
2. pozwalają na zmianę rozmiaru w czasie pracy systemu,
3. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
4. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
5. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 |
| 1. Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 |
| 1. Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 |
| 1. Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
 |
| 1. Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 |
| 1. Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 |
| 1. Graficzny interfejs użytkownika.
 |
| 1. Zlokalizowane w języku polskim, następujące elementy:
2. menu,
3. przeglądarka internetowa,
4. pomoc,
5. komunikaty systemowe.
 |
| 1. Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 |
| 1. Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 |
| 1. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
 |
| 1. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
 |
| 1. Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
2. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
3. 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:
4. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
5. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
6. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
7. zdalna dystrybucja oprogramowania na stacje robocze.
8. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
9. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
10. dystrybucję certyfikatów poprzez http,
11. konsolidację CA dla wielu lasów domeny.
12. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
13. szyfrowanie plików i folderów,
14. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
15. posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów,
16. serwis udostępniania stron WWW,
17. wsparcie dla protokołu IP w wersji 6 (IPv6),
18. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
19. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla:
20. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
21. obsługi ramek typu jumbo frames dla maszyn wirtualnych,
22. obsługi 4-KB sektorów dysków,
23. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra.
24. posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),
25. posiada 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.
 |
| 1. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 |
| 1. Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 |
| 1. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
 |
| 1. Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
 |

## 2.2 Systemy operacyjne dla serwerów bazodanowych – SSO2 BBB

|  |
| --- |
| LICENCJA SSO2 2 SZTUKI |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie** | Microsoft 2016 Standard 64bit z licencją obejmującą wszystkie cory procesora zainstalowanego w zaoferowanym serwerze bazodanowym: S4, S5 – licencja na nie mniej niż 16 core - w licencjonowaniu dla jednostek rządowych lub równoważne |
| **Inne** | Wykonawca zapewni 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. Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
2. Zamawiający wymaga typu licencji MOLP (Microsoft Open License Program) w licencjonowaniu dla jednostek rządowych.
3. 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 i nielimitowaną liczbę wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
 |

***Serwerowy System Operacyjny (SSO2) – opis równoważności:***

|  |
| --- |
| ***Wymagane minimalne parametry techniczne***  |
| 1. Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszta w przyszłym użytkowaniu.
2. Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).
3. 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 i dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
 |
| Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy. |
| 1. Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym
 |
| 1. Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
 |
| 1. Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
 |
| 1. Posiada 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.
 |
| 1. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 |
| 1. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 |
| 1. Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 |
| 1. Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 |
| 1. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
2. pozwalają na zmianę rozmiaru w czasie pracy systemu,
3. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
4. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
5. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 |
| 1. Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 |
| 1. Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 |
| 1. Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
 |
| 1. Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 |
| 1. Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 |
| 1. Graficzny interfejs użytkownika.
 |
| 1. Zlokalizowane w języku polskim, następujące elementy:
2. menu,
3. przeglądarka internetowa,
4. pomoc,
5. komunikaty systemowe.
 |
| 1. Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 |
| 1. Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 |
| 1. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
 |
| 1. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
 |
| 1. Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
2. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
3. 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:
4. podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
5. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
6. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
7. zdalna dystrybucja oprogramowania na stacje robocze.
8. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
9. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
10. dystrybucję certyfikatów poprzez http,
11. konsolidację CA dla wielu lasów domeny.
12. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
13. Szyfrowanie plików i folderów.
14. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
15. Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
16. Serwis udostępniania stron WWW.
17. Wsparcie dla protokołu IP w wersji 6 (IPv6),
18. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
19. 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:
20. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
21. obsługi ramek typu jumbo frames dla maszyn wirtualnych,
22. obsługi 4-KB sektorów dysków,
23. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra.
24. Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),
25. Posiada 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.
 |
| 1. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 |
| 1. Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 |
| 1. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
 |
| 1. Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
 |

## 2.3. Licencje dostępowe dla SSO

|  |
| --- |
| **LICENCJA SSO – CAL - 350 SZTUK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Oprogramowanie** | MS Windows 2016 Device CAL lub równoważne |
| **Inne** | Wykonawca zapewni 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 ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
3. Zamawiający wymaga typu licencji MOLP (Microsoft Open License Program) w licencjonowaniu dla jednostek rządowych.
4. Licencja ma 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 dla SSO – opis równoważności:***

|  |  |
| --- | --- |
| **Komponent** | **Minimalne wymagania** |
| **Sposób licencjonowania** | 1. Zamawiający nie dopuszcza licencji OEM.
2. Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
3. Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).
4. Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta.
5. Licencja ma umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.
 |
| **Cechy** | Licencja powinna 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. |

## 2.4 Motor bazy danych

|  |
| --- |
| **LICENCJA BAZY DANYCH - 2 SZTUKI** |
| **Wymagane minimalne parametry techniczne** |
| **Motor bazy danych musi wspierać systemy informatyczne ERP i LIS posiadane przez Zamawiającego.**  |
| 1. Wykonawca dostarczy odpowiednią liczbę licencji zgodną z ilością serwerów bazodanowych i zainstalowanych w nich procesorów.
 |
| 1. Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows i Linux.
 |
| 1. Oferowany Motor bazy danych musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych.
 |
| 1. Oferowany Motor bazy danych musi posiadać komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open-source.
 |
| 1. Oferowany Motor bazy danych ma mieć możliwość realizacji kopii bezpieczeństwa w trakcie działania (na gorąco).
 |
| 1. Oferowany Motor bazy danych ma umożliwiać generowanie kopii bezpieczeństwa automatycznie (o określonej porze) i na żądanie operatora oraz umożliwiać odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
 |
| 1. Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
 |
| 1. Administrator musi posiadać możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych).
 |
| 1. Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych.
 |
| 1. Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego.
 |
| 1. Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.
 |
| 1. Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.
 |
| 1. Wsparcie dla ustawień narodowych i zestawów znaków (włącznie z Unicode).
 |
| 1. Możliwość migracji zestawu znaków bazy danych do Unicode.
 |
| 1. Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
 |
| 1. Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych.
 |
| 1. Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych.
 |
| 1. Wsparcie protokołu XA
 |
| 1. Wsparcie standardu JDBC 3.0
 |
| 1. Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
 |
| 1. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
 |
| 1. Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu.
 |
| 1. Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej).
 |
| 1. Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych.
 |
| 1. Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.
 |
| 1. Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.
 |
| 1. Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online.
 |
| 1. Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup).
 |
| 1. Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.
 |
| 1. W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników.
 |
| 1. Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.
 |
| 1. Możliwość budowy klastra na węźle obsługiwanym przez maksymalnie 2 procesory.
 |

## 2.5 Oprogramowanie biurowe

|  |
| --- |
| **PAKIET OPROGRAMOWANIA BIUROWEGO - 40 SZTUK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Oprogramowanie biurowe** | 1. Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.:
2. edytor tekstów,
3. arkusz kalkulacyjny,
4. narzędzie do przygotowania i prowadzenia prezentacji,
5. narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
6. pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim,
7. powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa,
8. przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim,
9. dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego,
10. publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu,
11. możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).
12. Edytor tekstów musi umożliwiać:
13. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
14. wstawianie oraz formatowanie tabel,
15. wstawianie oraz formatowanie obiektów graficznych,
16. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
17. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
18. automatyczne tworzenie spisów treści,
19. formatowanie nagłówków i stopek stron,
20. śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
21. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
22. określenie układu strony (pionowa/pozioma),
23. wydruk dokumentów,
24. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
25. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
26. Arkusz kalkulacyjny musi umożliwiać:
27. tworzenie raportów tabelarycznych,
28. tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
29. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
30. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),
31. obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych,
32. narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
33. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
34. wyszukiwanie i zamianę danych,
35. wykonywanie analiz danych przy użyciu formatowania warunkowego,
36. nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
37. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
38. formatowanie czasu, daty i wartości finansowych z polskim formatem,
39. zapis wielu arkuszy kalkulacyjnych w jednym pliku,
40. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
41. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
42. przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego,
43. drukowanie w formacie umożliwiającym robienie notatek,
44. zapisanie jako prezentacja tylko do odczytu,
45. nagrywanie narracji i dołączanie jej do prezentacji,
46. opatrywanie slajdów notatkami dla prezentera,
47. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
48. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
49. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
50. możliwość tworzenia animacji obiektów i całych slajdów,
51. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

5. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:1. pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
2. przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
3. filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
4. tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
5. automatyczne grupowanie poczty o tym samym tytule,
6. tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
7. oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
8. mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
9. zarządzanie kalendarzem,
10. udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
11. przeglądanie kalendarza innych użytkowników,
12. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
13. zarządzanie listą zadań,
14. zlecanie zadań innym użytkownikom,
15. zarządzanie listą kontaktów,
16. udostępnianie listy kontaktów innym użytkownikom,
17. przeglądanie listy kontaktów innych użytkowników,
18. możliwość przesyłania kontaktów innym użytkowników.
 |

## 2.6 Oprogramowanie antywirusowe

Zamawiający obecnie używa 300 licencji oprogramowania antywirusowego G DATA ENDPOINT PROTECTION BUSINESS z aktywnym serwisem do 31-03-2020 roku. Wykonawca musi dostarczyć oprogramowanie antywirusowe na 350 stanowisk spełniające poniższe wymagania funkcjonalne, z uwzględnieniem posiadanych przez Szpital licencji, z ważnością subskrypcji na 3 lata od dnia 31-03-2020 roku.

|  |
| --- |
| **OPROGRAMOWANIE ANTYWIRUSOWE -350 SZTUK** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Specyfikacja produktowa oprogramowania antywirusowego chroniącego stacje****robocze i serwery plików** | 1. Pełne wsparcie dla systemu Windows: 10, 8.x, 7, Vista, Server 2016, Server 2012, Server 2008, 2003 Server.
2. Wsparcie dla systemów XP SP3 32-bit, Linux 32/64-bit, OS X (tylko klient).
3. Interfejsy programu, pomoce i podręczniki w języku polskim.
4. Pomoc techniczna w języku polskim.
5. Potwierdzona średnia skuteczność oprogramowania we wszystkich testach „File Detection Test of Malicious Software” z roku 2012 i 2013 przeprowadzonych przez organizację AV-Comparatives przynajmniej na poziomie 99,5% wykrytych zagrożeń.
 |
| **Ochrona antywirusowa** | 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
3. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
4. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.
5. Klient oprogramowania antywirusowego dla linuksowych serwerów Samba.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Dwa niezależne skanery antywirusowe (nie heurystyczne!) z dwoma niezależnymi bazami
8. sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej.
9. Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami antywirusowymi jednocześnie.
10. Dodatkowy i niezależny od skanerów plików, trzeci skaner poczty oparty o technologię cloud security.
11. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów,
12. plików lub procesów.
13. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików
14. na żądanie lub według harmonogramu.
15. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rodzaj plików do skanowania, priorytet skanowania).
16. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
17. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy
18. czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.
19. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
20. Możliwość skanowania dysków sieciowych i dysków przenośnych.
21. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
22. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
23. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
24. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
25. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
26. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
27. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
28. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
29. Dodatek do aplikacji MS Outlook umożliwia ponowne skanowanie wszystkich nieprzeczytanych wiadomość znajdujących się w skrzynce
30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
31. Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z bankami i sklepami online.
32. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
33. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
34. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
35. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
36. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do
37. dowolnej stacji roboczej w sieci lokalnej.
38. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
39. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
40. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
43. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).
44. Program wyposażony w tylko w jeden serwer skanujący uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).
45. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
46. Kontrola zachowania aplikacji (Behaviour Blocking) do wykrywania podejrzanie zachowujących się aplikacji.
47. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on używany.
48. Ochrona przed urządzeniami podszywającymi się po klawiatury USB.
49. Moduł do ochrony przed exploitami (ataki 0-day).
50. Ochrona stacji Windows przed spamem z możliwością tworzenia białych i czarnych list adresów/domen.
 |
| **Zdalne administrowanie ochroną** | 1. Integracja z Active Directory – import kont komputerów i jednostek organizacyjnych.
2. Ochrona dla urządzeń z systemem Android.
3. Zarządzanie urządzeniami z systemem iOS.
4. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich
5. podłączonych komputerach Active Directory.
6. Zdalna instalacja i centralne zarządzanie klientami na stacjach roboczych i serwerach Windows.
7. Zdalna instalacja i centralne zarządzanie klientami Linux / OS X.
8. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.
9. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli (przynajmniej aktualizacje, ochronę przeglądarek, skanowania zasobów, synchronizacji raportów).
10. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
11. Możliwość eksportu/importu ustawień dla stacji/grupy stacji.
12. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.
13. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.
14. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).
15. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
16. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
17. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez przeglądarki internetowe (z sieci lokalnej i spoza niej).
18. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez urządzenia mobilne (smartfony, tablety) oparte o system Android (z sieci lokalnej i spoza niej).
19. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.
20. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
21. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
22. Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach (nazwa, wersja, producent, data instalacji).
23. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.
24. Odczyt informacji o zasobach sprzętowych stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku/partycji systemowej).
25. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
26. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
27. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
28. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
29. Możliwość generowania raportów w formacie XML.
30. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów.
31. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych.
32. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji roboczej.
33. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych.
34. Możliwość dynamicznego grupowania stacji na podstawie parametrów: nazwa komputera, adres IP, brama domyślna, nazwa domeny.
 |
| **Raporty** | 1. Możliwość utworzenia raportów statusu ochrony sieci.
2. Możliwość generowania raportów w przynajmniej 3 językach.
3. Możliwość wysyłania raportów z określonym interwałem.
4. Możliwość wysłania jednego raportu na różne adresy mailowe lub grupy adresów.
5. Możliwość zdefiniowania przynajmniej 15 różnych typów informacji dotyczących statusu ochrony oraz różnych form ich przedstawienia (tabele, wykresy) w pojedynczym raporcie.
 |
| **Osobista zapora połączeń sieciowych** | 1. W pełni zdalna instalacja, zdalne zarządzanie wszystkimi funkcjami zapory i zdalna deinstalacja.
2. Zapora działająca domyślnie trybie automatycznego rozpoznawania niegroźnych połączeń i tworzenia reguł bez udziału użytkownika.
3. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
4. Możliwość interakcji między użytkownikiem a administratorem w celu dostosowania zestawu reguł.
5. Możliwość zdefiniowania osobnych zestawów reguł dla dowolnych grup użytkowników.
6. Wbudowany system IDS.
7. Możliwość pracy w trybie offsite, po odłączeniu od sieci przedsiębiorstwa.
8. Wykrywanie zmian w aplikacjach korzystających z sieci na podstawie sum kontrolnych i monitorowanie o tym zdarzeniu.
9. Możliwość automatycznego skanowania antywirusowego modułów o zmodyfikowanych sumach kontrolnych.
10. Automatyczne wysyłanie powiadomień o zablokowaniu aktywności sieciowej na wskazany adres mailowy.
11. Import/eksport reguł/zestawów reguł zapory na stacji roboczej
 |
| **Zdalne zarządzanie wydajnością i czasem pracowników (PolicyManager)** | 1. Wszystkie obostrzenia modułu można zastosować zarówno wobec użytkowników z ograniczonymi kontami Windows, jak i administratorów.
2. Kontrola aplikacji umożliwiająca blokowanie lub zezwalanie na stosowanie konkretnych programów, folderów i plików. Opcja zablokowania pliku w konkretnej wersji, o danej sumie kontrolnej oraz podpisanego cyfrowo przez wskazanego producenta.
3. Kontrola urządzeń pozwalająca na zarządzanie dostępem do napędów CD/DVD/BD, pendrive’ów, dysków oraz kamer USB, a także tradycyjnych stacji dyskietek.
4. Możliwe jest zablokowanie urządzenia a także ustawienie dostępu tylko do odczytu.
5. Możliwość wykluczenia urządzeń na podstawie ich numeru ID i nadanie im pełnych uprawnień lub tylko do odczytu.
6. W przypadku wykluczeń urządzeń możliwe jest napisanie odpowiedniego komentarza dla danego wyjątku.
7. Kontrola treści internetowych umożliwiająca zablokowanie/odblokowanie użytkownikom stron internetowych z konkretnych kategorii. Rozbudowana lista aktualizowana jest przez Internet.
8. Biała i czarna lista stron internetowych stosowana bez względu na przypisaną im kategorię treści.
9. Kontrola czasu spędzanego w Internecie. Możliwość precyzyjnego określenia w jakich godzinach jakiego dnia użytkownik może przeglądać treści internetowe. Dodatkowo można określić dzienny, tygodniowy oraz miesięczny limit czasu przeznaczonego do korzystania ze stron internetowych.
10. Po zablokowaniu aplikacji, urządzenia lub strony internetowej użytkownik może zażądać udostępnienia zablokowanego zasobu wprost z okna z komunikatem o blokadzie.
11. Administrator ma możliwość odblokowania zasobu z poziomu raportu konsoli zarządzającej utworzonego automatycznie po zaznaczeniu przez użytkownika opcji zażądania dostępu do zablokowanego zasobu.
12. Automatyczne wysyłanie powiadomień o zablokowaniu danego zasobu na wskazany adres mailowy.
 |

# Systemy backupu i archiwizacji

## Biblioteka taśmowa

|  |
| --- |
| **BIBLIOTEKA TAŚMOWA - 1 SZTUKA** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| **Obudowa** | Do zamontowania w szafie rack, maksymalnie 1U |
| **Napęd** | 1. Wyposażony w co najmniej 1 sztukę napędów, o parametrach:
2. standard LTO7 lub lepszy – interfesj SAS,
3. w komplecie kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m.
4. Dodatkowo:
5. 60 sztuk etykiet LTO7,
6. 25 taśm LTO7,
7. taśma czyszcząca.
 |
| **Liczba slotów** | Co najmniej 9 slotów przeznaczonych na zestaw taśm. |

## Oprogramowanie do backupu

Przewidywany model wykonywania backupu to disk to disk to tape (D2D2T). Oznacza to, że dane produkcyjne zostaną odseparowane od miejsca składowania backupu. Dane produkcyjne zostaną zlokalizowane na macierzy dyskowej MD1 z MRM2, natomiast backup będzie wykonywany na dyski zainstalowane w istniejącym NAS-ie Synology RS2416RP+ (dysku sieciowym zlokalizowanym w Serwerowni zapasowej). Następnie będą backupowane dana na bibliotece taśmowej.

|  |
| --- |
| **OPROGRAMOWANIE DO BACKUPU – 1 KOMPLET** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Wykonawca dostarczy licencje na oprogramowanie do backupu obejmujące co najmniej środowisko:1.1. Serwerów wirtualizacyjnych S1, S2, S3 - środowisko fizyczne i wirtualne1.2. Serwerów bazodanowych S4, S5 - środowisko fizyczne1.3. Istniejącego serwera HIS bazodanowego – środowisko fizyczne systemu WindowsW przypadku zaoferowania większej ilości serwerów przez Wykonawcę, należy objąć wszystkie nowe serwery oprogramowaniem backupowym.  |
| **Funkcjonalność** | 1. Oprogramowanie ma obsługiwać urządzenia taśmowe i dyskowe, służące do przechowywania kopii zapasowych danych.
2. Oprogramowanie musi posiadać architekturę min. 2 warstwową z wydzielonym centralnym serwerem backupowym.
3. Oprogramowanie musi posiadać graficzny interfejs zarządzania.
4. Oprogramowanie ma umożliwiać definiowanie w sposób centralny z jednej konsoli procesów polityki tworzenia kopii zapasowych, tj. określenia, jakie dane, kiedy i gdzie powinny być składowane (definiowanie, planowanie i zarządzanie harmonogramu backupu).
5. Oprogramowanie ma umożliwiać realizowanie raz zdefiniowanej polityki backupu w sposób automatyczny.
6. Oprogramowanie ma umożliwiać tworzenie kopii zapasowych on-linie serwerów bazodanowych bez konieczności zatrzymywania pracy serwera bazy danych.
7. Oprogramowanie ma posiadać moduł monitorowania i raportowania systemu backupu.
8. Oprogramowanie ma umożliwiać na definiowanie kryteriów alarmów systemu backupu.
9. Program powinien umożliwiać szyfrowanie archiwów AES z co najmniej 256 bitowym kluczem szyfrującym
10. Program powinien umożliwiać wyszukiwanie plików w kopiach zapasowych.
 |
| **Kopie zapasowe** | 1. Kopie zapasowe całych dysków i partycji.
2. Kopie zapasowe wybranych plików i folderów.
3. Możliwość tworzenia kopii zapasowych plików otwartych.
4. Kopie zapasowe aplikacji (Exchange, SharePoint, Active Directory).
5. Kopie zapasowe baz danych Oracle, MS SQL, MySQL.
6. Kopie zapasowe całych maszyn wirtualnych.
7. Zapis kopii zapasowych na udziały sieciowe oraz inne nośniki (dyski, napęd taśmowy).
 |
| **Odtwarzanie** | 1. Odtworzenie poszczególnych plików i folderów.
2. Odtworzenie całej maszyny.
3. Odtwarzanie baz danych Oracle, Microsoft SQL.
4. Odtwarzanie kontrolerów domeny Microsoft Active Directory.
 |
| **Licencjonowanie** | Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych i ilość maszyn wirtualnych.  |

# Systemy bezpieczeństwa

## Wdrożenie AD

1. Utworzenie dwóch maszyn wirtualnych w ramach klastra pracy awaryjnej wraz z instalacją i aktualizacją systemów operacyjnych Windows na maszynach pracujących w klastrze HA – Serwery S1, S2, S3.
2. Wypromowanie nowej domeny Active Directory i utworzenie 650 kont użytkowników z listy dostarczonej przez Szpital (schemat listy zostanie dostarczony przez Szpital) oraz podłączenie serwerów do bieżącej struktury Active Directory.
3. Skonfigurować serwer WSUS do aktualizacji systemów operacyjnych stacji roboczych.
4. Podpięcie do domeny 20 wskazanych przez pracowników Szpitala stacji roboczych wraz z pokazaniem migracji pulpitów użytkowników.  Zamawiający podepnie pozostałe komputery do domeny zgodnie z instrukcjami wykonawcy
5. Wykonawca wykona 8 godzinne szkolenie z administrowania dostarczonym rozwiązaniem.

## System zarządzania infrastrukturą IT

|  |
| --- |
| **SYSTEM ZARZĄDZANIA INFRASTRUKTURĄ IT - 1 KOMPLET** |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Wykonawca dostarczy:1. 350 licencji wieczystych do zarządzania infrastrukturą IT,
2. 4 konsole dostępowe,
3. Co najmniej jednodniowe wdrożenie,
4. Co najmniej jednodniowe szkolenie w siedzibie,
5. pięcioletnie wsparcie z aktualizacjami do systemu.
 |
| **Wymagania Ogólne** | 1. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 350 stanowisk komputerowych oraz nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto muszą posiadać co najmniej 4 licencje dostępowe do konsoli zarządzającej
 |
| 1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
 |
| 1. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
 |
| 1. Oprogramowanie serwera aplikacji musi umożliwiać dystrybucję zadań oraz plików wg zaprojektowanej trasy przepływu danych z dedykowanego dla każdej lokalizacji repozytorium plików.
 |
| 1. Oprogramowanie musi umożliwiać zaprojektowanie drzewiastej struktury przepływu danych (trasy) pomiędzy agentami a centralnym serwerem systemu.
 |
| 1. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta poprzez lokalny odczyt WMI oraz bezpośredni dostęp do komponentów np. bezpośredni odczyt parametrów z BIOS’u komputera.
 |
| 1. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do szyfrowanego pliku.
 |
| 1. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
 |
| 1. Oprogramowanie musi posiadać sprzętową obsługę jednoczesnych sesji operatorów konsoli (licencja pływająca) umożliwiającą jednoczesną pracę n-operatorów na wybranych instancjach zainstalowanych konsol zarządzających.
 |
| 1. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
 |
| 1. Oprogramowanie musi współpracować z serwerem MsSQL Server 2005/2008/2008R2/2012/2014.
 |
| 1. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
 |
| 1. Oprogramowanie musi posiadać przypisywanie wybranych jednostek organizacyjnych, Jednostek Lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych widoków drzewiastych z danych dostępnych w systemie. Jeśli obiekt systemu jest w relacji z innym obiektem, to musi być możliwość zaprezentowania go w strukturze drzewa.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie kolumn w strukturze drzewiastej, w której jest możliwość umieszczenia dowolnej danej związanej z obiektem.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie wyrażeń w zakresie co najmniej funkcji zliczania obiektów podrzędnych wybranego typu w strukturze drzewiastej oraz sumowania ich wybranej właściwości liczbowej.
 |
| 1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych zbudowanych struktur widoków drzewiastych i udostępniania ich innym użytkownikom systemu.
 |
| 1. Oprogramowanie musi umożliwiać eksport do Excela widoku drzewiastego od dowolnego obiektu w głąb, umożliwiając wybór konkretnych typów obiektów do eksportu.
 |
| 1. Oprogramowanie musi być podpisane cyfrowo przez producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy każdego składnika Producenta systemu włączając w to pliki wykonywalne (\*.exe), pliki bibliotek współdzielonych (\*.dll), pliki sterowników (\*.sys) oraz pliki paczek oprogramowania (\*.msi).
 |
| 1. Oprogramowanie musi realizować bezpośrednie zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej bez użycia wywoływanych widocznych interfejsów WWW.
 |
| 1. Oprogramowanie agenta musi realizować wszystkie wymagane funkcjonalności za pomocą aplikacji lub usług wyprodukowanych i podpisanych cyfrowo przez Producenta bez użycia aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
 |
| 1. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
 |
| 1. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min. : Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
 |
| 1. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
 |
| 1. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, grupy agentów, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
 |
| 1. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/LDAP), kont użytkowników oraz komputerów wraz z zachowaniem ich oryginalnego położenia z możliwością tworzenia listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
 |
| 1. Oprogramowanie musi posiadać kreator powiązań dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
 |
| 1. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
 |
| 1. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
 |
| 1. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
 |
| 1. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
 |
| 1. Oprogramowanie musi umożliwiać automatyczny odczyt informacji nt. uprawnień (ACL) do wybranych folderów z określonych grup stanowisk komputerowych (raport wg struktury organizacyjnej lub lokalizacyjnej).
 |
| 1. Oprogramowanie musi umożliwiać automatyczny odczyt informacji nt. aktywnych lokalnych kont administracyjnych z określonych grup stanowisk komputerowych (raport wg struktury organizacyjnej lub lokalizacyjnej).
 |
| 1. Oprogramowanie musi umożliwiać globalne uruchamianie skryptów PowerShell na wybranych grupach stanowisk komputerowych (wg struktury organizacyjnej lub lokalizacyjnej).
 |
| 1. W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.
 |
| 1. Zamawiający wymaga od wykonawcy aby dostarczył i zdalnie wdrożył oprogramowanie w terminie do 30 dni od podpisania umowy w zakresie :
2. Analiza przedwdrożeniowa,
3. Instalacja oraz konfiguracja bazy danych,
4. Instalacja oraz konfiguracja głównej konsoli zarządzającej,
5. Instalacja oraz konfiguracja usługi serwera aplikacji,
6. Instalacja oraz konfiguracja pomocniczych serwerów (local site servers),
7. Określenie parametrów pracy agentów systemu,
8. Integracja informacji z Active Directory,
9. Konfiguracja uprawnień dla użytkowników konsol zarządzających,
10. Przygotowanie skonfigurowanej paczki agenta,
11. Sprawdzenie poprawności instalacji agenta,
12. Manualna instalacja agenta systemu dla testowej grupy użytkowników (maksymalnie 5 stacji) celem sprawdzenia poprawności komunikacji z bazą danych oraz konsolami zarządzającymi,
13. Sprawdzenie poprawności działania wdrożonych funkcji systemu.
14. Zamawiający wymaga od wykonawcy aby przeprowadził jedno szkolenie dla administratorów systemu w zakresie administracji systemem w siedzibie zamawiającego (wymagana 1 sesja co najmniej 4 godzinna)
 |
| **Wymagany zakres funkcjonalny systemu** | 1. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
 |
| 1. Oprogramowanie musi umożliwiać analizę sprzętową:
2. płyty głównej w zakresie model, producent, nr. seryjny,
3. CPU w zakresie nazwy, modelu, producenta, częstotliwości,
4. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
5. RAM w zakresie wielkości pamięci,
6. karty sieciowej w zakresie model, adres IP, adres MAC,
7. karty graficznej w zakresie model.
 |
| 1. Oprogramowanie musi posiadać wbudowany alerter, którego zadaniem jest cykliczne informowanie (poprzez e-mail) administratorów systemu o zmianach w zakresie konfiguracji sprzętowej, zmianach w oprogramowaniu (instalacja, dezinstalacja), kończących się okresach gwarancji zarządzanych zasobów (komputery, urządzenia dodatkowe), wygasaniu licencji na oprogramowanie, informacje o planowanych przeglądach serwisowych, obciążenie pamięci RAM oraz zajętość dysków twardych.
 |
| 1. Oprogramowanie musi posiadać filtry aktywności pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3 bez konieczności fizycznej obecności użytkownika przy stacji.
 |
| 1. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
 |
| 1. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
 |
| 1. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
 |
| 1. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
 |
| 1. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
 |
| 1. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
 |
| 1. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
 |
| 1. Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów
 |
| 1. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
 |
| 1. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie : operator, data, czas, poprzednia oraz nowa wartość.
 |
| 1. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
 |
| 1. Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów.
 |
| 1. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
 |
| 1. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
 |
| 1. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
 |
| 1. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
 |
| 1. Oprogramowanie musi umożliwiać wykrywanie zmian w konfiguracji sprzętowej komputerów.
 |
| 1. Oprogramowanie musi umożliwiać zapis dodatkowych informacji inwentaryzacyjnych dotyczących całego stanowiska komputerowego w zakresie numeru seryjnego komputera, numeru seryjnego monitora, numeru seryjnego drukarki, numeru seryjnego dowolnych urządzeń peryferyjnych,
 |
| 1. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
 |
| 1. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
 |
| 1. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
 |
| 1. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie : model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
 |
| 1. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie : numer faktury, numer seryjny, model, nazwa, data zakupu.
 |
| 1. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
 |
| 1. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
 |
| 1. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
 |
| 1. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie zestawień duplikatów kluczy licencyjnych dotyczących zainstalowanego oprogramowania na komputerze.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
 |
| 1. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
 |
| 1. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem (wymagana w organizacji) wraz z możliwością raportowania wg w/w klasyfikacji.
 |
| 1. Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
 |
| 1. Oprogramowanie musi umożliwiać analizę (aktualna oraz historyczna) średniego obciążenia CPU oraz transferu IO przez dowolnie wybrany proces w zadanych czasookresie.
 |
| 1. Oprogramowanie musi umożliwiać zapisywanie informacji o procesach w bazie danych i powinny zawierać następujące informacje: nazwa procesu, lokalizacja, zajmowana pamięć, nazwa stanowiska gdzie po raz pierwszy wystąpił proces, data i czas wykrycia.
 |
| 1. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
 |
| 1. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury katalogowej, struktury sieciowej (pule IP) oraz własnego podziału.
 |
| 1. Oprogramowanie musi umożliwiać dynamiczne zawężania wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
 |
| 1. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
 |
| 1. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
 |
| 1. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
 |
| 1. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
 |
| 1. Oprogramowanie musi umożliwiać całkowitą interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska administratora stanowiska użytkownika, bez konieczności uprzedniego wylogowania użytkownika.
 |
| 1. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego.
 |
| 1. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
 |
| 1. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
 |
| 1. Oprogramowanie musi umożliwiać zdalną dwukierunkową linie poleceń.
 |
| 1. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
 |
| 1. Oprogramowanie musi umożliwiać zdalną instalację pakietów \*.msi, plików \*.cmd, \*.bat, \*.reg poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
 |
| 1. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
 |
| 1. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
 |
| 1. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
 |
| 1. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych „local site servers”) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
 |
| 1. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
 |
| 1. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
 |
| 1. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
 |
| 1. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
 |
| 1. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
 |
| 1. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
 |
| 1. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.
 |
| 1. Oprogramowanie musi umożliwiać generowanie wybranych raportów do pliku: PDF, CSV i Excel.
 |
| 1. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).
 |
| 1. Oprogramowanie musi umożliwiać globalny przegląd stanu zajętości dysków, obciążenia pamięci RAM oraz CPU w formie graficznych wykresów obejmujących wszystkie zarejestrowane w systemie stanowiska.
 |
| 1. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem z zapisem historii konwersacji.
 |
| 1. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
 |
| 1. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
 |
| 1. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
 |
| 1. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
 |
| 1. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
 |
| 1. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
 |
| 1. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
 |
| 1. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
 |
| 1. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
 |
| 1. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
 |
| 1. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi
2. odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem
3. wydruków dla drukarki lokalnej.
 |
| 1. Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, rozmiar drukowanych stron.
 |
| 1. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).
 |
| 1. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
 |
| 1. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
 |
| 1. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. \*.doc, które mają być archiwizowane.
 |
| 1. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
 |
| 1. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
 |
| 1. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
 |
| 1. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.
 |
| 1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.
 |
| 1. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB.
 |
| 1. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
 |
| 1. Oprogramowanie musi umożliwiać autoryzację wybranych urządzeń USB.
 |
| 1. Oprogramowanie musi posiadać filtry aktywności pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3 bez konieczności fizycznej obecności użytkownika przy stacji.
 |
| 1. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
 |
| 1. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu : Grupa\Stanowisko\Zalogowany Użytkownik.
 |
| 1. Oprogramowanie musi umożliwiać filtrację okresową oraz wg grup stanowisk.
 |

# Szkolenia

## Szkolenie informatyczne (infrastruktura IT)

Zakres szkoleń dla 4 Informatyków musi obejmować co najmniej następujące zagadnienia:

1. System wirtualizacji – podstawowe szkolenie z instalacji, konfiguracji i zarządzania.
2. System operacyjny serwerowy – podstawowe szkolenia z instalacji, konfiguracji i zarządzania podstaw usług sieciowych, wdrożenia i konfiguracji usług katalogowych.
3. Urządzenia do ochrony brzegu sieci - podstawowe szkolenie z instalacji, konfiguracji i zarządzania.
4. Oprogramowanie do zarządzania siecią przewodową i bezprzewodową – podstawowe szkolenie z instalacji, konfiguracji i zarządzania.
5. Oprogramowanie do zarządzania infrastrukturą teleinformatyczną - podstawowe szkolenie z instalacji, konfiguracji i zarządzania.
6. Antywirus – podstawowe szkolenie z instalacji, konfiguracji i zarządzania.
7. Serwer bazodanowy - podstawowe szkolenie z instalacji, konfiguracji i zarządzania.
8. Administrowania środowiskiem serwerowo-macierzowym:
9. prezentacja dostarczonych produktów;
10. omówienie architektury wdrożonego środowiska;
11. omówienie zasad i procedur administrowania w tym konfiguracji urządzeń i środowiska,
12. wirtualizacji oraz monitorowania środowiska;
13. Administrowania kopią bezpieczeństwa (backupu):
14. prezentacja dostarczonego oprogramowania na potrzeby backupu;
15. omówienie architektury wdrożonego rozwiązania backupu;
16. omówienie konfiguracji backup;
17. przedstawienie zasad i procedur administrowania i monitorowania pracy podsystemu backupu;
18. Administrowania systemem wirtualizacji:
19. omówienie architektury;
20. administracja systemu;
21. monitoring;
22. Administrowania sieci informatycznej:
23. prezentacja dostarczonych urządzeń sieciowych;
24. zapoznanie z systemem operacyjnym urządzeń;
25. omówienie konfiguracji środowiska;
26. przedstawienie zasad i procedur administrowania i monitorowania pracy środowiska sieciowego;