**Załącznik 5b do SIWZ**

**Opis przedmiotu zamówienia**

**Dostawa i instalacja sprzętu aktywnego, serwerowego i komputerowego wraz z oprogramowaniem.**

**Opis przedmiotu zamówienia**

Przedmiot zamówienia obejmuje dostawę zgodnie z poniższym wykazem:

|  |  |
| --- | --- |
| 1. **Przełącznik LAN 48-portowy – 2 sztuki**   **(miejsce instalacji: serwerownia w budynku Urzędu Miejskiego w Olecku przy Placu Wolności 3)** | |
| **Nazwa składnika/parametru technicznego sprzętu** | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |

|  |  |
| --- | --- |
| Ilość i typ portów | Minimum 48 portów 100BaseTX/1000BaseT z autonegocjacją  (zgodność z IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T: tylko pełny duplex;)  Minimum 4 porty SFP/SFP+  1 port szeregowy konsoli RJ45 lub USB |
| Parametry wydajnościowe | Warstwa przełączania: 3  Tablica routingu: 10000 wpisów (IPv4), 5000 wpisów (IPv6),  Prędkość magistrali: 175 Gbps  Przepustowość: 110 Mpps  Ilość wpisów tablicy adresów MAC: min. 32000  Opóźnienie: <3.8 µs dla 1000 Mbit  Ilość obsługiwanych VLAN-ów: min. 512 (802.1q) |
| Zarządzanie | CLI, SSH, WWW, telnet.  Dedykowany port konsolowy do zarządzania poza pasmowego, w pełni niezależny od portów liniowych.  Możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo. |
| Procesor i pamięć | Taktowanie procesora min. 1000MHz  min. 4GB pamięci flash  min. 1GB DDR3 pamięci RAM |
| Funkcje wysokiej dostępności | Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s), RPVST+ |
| Funkcje stackowania | Obsługa VSF(Virtual Switching Framework) do czterech urządzeń w stosie przez dowolny port uplink |
| Agregacja portów | zgodna z 802.3ad LACP |
| QoS | priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek, rate-limiting, algorytm opróżniania kolejek WDRR i SP, Voice VLAN, Layer 4 prioritization, Class of Service (CoS) |
| Monitorowanie | RMON 4 grupy statistics, history, alarm, events, SFLOW |
| Oprogramowanie | Aktualizacje dostępne na stronie producenta |
| Pozostałe funkcje | LLDP,LLDP-MED, dual flash images, obsługa ramek typu Jumbo, DHCP snooping, DHCP Server, BPDU Guard, BPDU Protection, izolacja portów, wsparcie dla IPv4 i Ipv6, Tunneled node dla ruchu z AP, Zero Touch Provisioning, wsparcie dla VRRP, obsługa GVRP and MVRP |
| Obudowa | Umożliwiająca instalację w szafie 19". Wysokość max. 1U. |
| Moc pobierana maksymalna | 50W, zasilacz z certyfikatem 80 PLUS Silver |
| Zasilanie | 200 - 240 VAC |
| Środowisko pracy | 0°C do 45°C |
| Wyposażenie (dostarczone w komplecie z 2 przełącznikami) | a) Kabel konsolowy.  b) Wyposażenie do połącznia przełączników (stackowania) o przepływności co najmniej 10Gbit/s z wykorzystaniem portów SFP+  c) Wyposażenie do podłączenia przełącznika 48-portowego PoE+ interfejsem 1Gbit/s z wykorzystaniem portów SFP/SFP+ (do połączenia przełączników nie dopuszcza się wykorzystywania portów 100BaseTX/1000BaseT)  d) Komplet wkładek (2 szt.) SFP 1G na światłowód wielomodowy o zasięgu do 500m oraz patchcordy optyczne (2 szt.) do zestawienia podłączenia pomiędzy budynkami Plac Wolności 3 i Plac Wolności 1 z dostarczanego przełącznika LAN 48-portowego do istniejącego przełącznika 48 100/1000 BaseT + 4SFP (posiadanego przez Zamawiającego), który w ramach realizacji przedmiotu zamówienia Wykonawca przeniesie, zainstaluje, uruchomi i skonfiguruje w budynku Urzędu Miejskiego przy Placu Wolności 1. Ponadto Zamawiający informuje, że posiada 2 komplety wkładek SFP 1Gbit/s na światłowód wielomodowy przeznaczonych odpowiednio do posiadanych przełączników HP i Cisco, które mogą być wykorzystane, o ile będą pasowały technicznie do dostarczanego przełącznika.  e) Wyposażenie do wykonania 4 połączeń z przełączników 48-portowych do serwerów o przepływności co Ethernet 10Gbit/s z wykorzystaniem portów SFP+ w przełącznikach (do połączenia serwerów do przełączników nie dopuszcza się wykorzystywania portów 100BaseTX/1000BaseT przełączników i serwerów). |
| Gwarancja | Dożywotnia (tak długo jak Zamawiający posiada produkt) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |

|  |  |
| --- | --- |
| 1. **Przełącznik LAN 48-portowy PoE+ – 1 sztuki**   **(miejsce instalacji: serwerownia w budynku Urzędu Miejskiego w Olecku przy Placu Wolności 3)** | |
| **Nazwa składnika/parametru technicznego sprzętu** | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |

|  |  |
| --- | --- |
| Ilość i typ portów | Minimum 48 portów 100BaseTX/1000BaseT z autonegocjacją i wsparciem dla standardu 802.3at PoE+  (zgodność z IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T, IEEE 802.3at PoE+); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T: tylko pełny duplex)  Minimum 4 porty SFP  1 port szeregowy konsoli RJ45 lub USB |
| Parametry wydajnościowe | Warstwa przełączania: 3  Tablica routingu: 10000 wpisów (IPv4), 5000 wpisów (IPv6)  Prędkość magistrali: 102 Gbps  Przepustowość: 76 Mpps  Ilość wpisów tablicy adresów MAC: min. 32000  Opóźnienie: <3.8 µs dla 1000 Mbit  Ilość obsługiwanych VLAN-ów: min. 512 (802.1q) |
| Zarządzanie | CLI, SSH, WWW, telnet.  Dedykowany port konsolowy do zarządzania poza pasmowego, w pełni niezależny od portów liniowych.  Możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo. |
| Procesor i pamięć | Taktowanie procesora min. 1000MHz  min. 4GB pamięci flash  min. 1GB DDR3 pamięci RAM |
| Funkcje wysokiej dostępności | Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s), RPVST+ |
| Funkcje stackowania | Obsługa VSF(Virtual Switching Framework) do czterech urządzeń w stosie przez dowolny port uplink |
| Agregacja portów | zgodna z 802.3ad LACP |
| QoS | priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek, rate-limiting, algorytm opróżniania kolejek WDRR i SP, Voice VLAN, Layer 4 prioritization, Class of Service (CoS) |
| Monitorowanie | RMON 4 grupy statistics, history, alarm, events, SFLOW |
| Oprogramowanie | Aktualizacje dostępne na stronie producenta |
| Pozostałe funkcje | LLDP,LLDP-MED, dual flash images, obsługa ramek typu Jumbo, DHCP snooping, DHCP Server, BPDU Guard, BPDU Protection, izolacja portów, wsparcie dla IPv4 i Ipv6, Tunneled node dla ruchu z AP, Zero Touch Provisioning, wsparcie dla VRRP, obsługa GVRP and MVRP |
| Obudowa | Umożliwiająca instalację w szafie 19". Wysokość max. 1U. |
| Moc pobierana maksymalna | 470W, zasilacz z certyfikatem 80 PLUS Silver |
| Zasilanie | 200 - 240 VAC |
| Środowisko pracy | 0°C do 45°C |
| Gwarancja | Dożywotnia (tak długo jak Zamawiający posiada produkt) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |

|  |  |
| --- | --- |
| 1. **Przełącznik LAN 24-portowy PoE+ – 1 sztuki**   **(miejsce instalacji: budynek Urzędu Miejskiego w Olecku przy Placu Wolności 1)** | |
| **Nazwa składnika/parametru technicznego sprzętu** | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |

|  |  |
| --- | --- |
| Ilość i typ portów | Minimum 24 porty 100BaseTX/1000BaseT z autonegocjacją i wsparciem dla standardu 802.3at PoE+  (zgodność z IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T, IEEE 802.3at PoE+); duplex 10Base-T/100Base-TX: pół lub pełny duplex; 1000Base-T: tylko pełny duplex)  Minimum 4 porty SFP  1 port szeregowy konsoli RJ45 lub USB |
| Parametry wydajnościowe | Warstwa przełączania: 3  Tablica routingu: 10000 wpisów (IPv4), 5000 wpisów (IPv6)  Prędkość magistrali: 55 Gbps  Przepustowość: 40 Mpps  Ilość wpisów tablicy adresów MAC: min. 32000  Opóźnienie: <3.8 µs dla 1000 Mbit  Ilość obsługiwanych VLAN-ów: min. 512 (802.1q) |
| Zarządzanie | CLI, SSH, WWW, telnet.  Dedykowany port konsolowy do zarządzania poza pasmowego, w pełni niezależny od portów liniowych.  Możliwość scentralizowanego zarządzania zarówno przez dedykowane oprogramowanie producenta jak i chmurowo  Kabel konsolowy dostarczony razem z przełącznikiem. |
| Procesor i pamięć | Taktowanie procesora min. 1000MHz  min. 4GB pamięci flash  min. 1GB DDR3 pamięci RAM |
| Funkcje wysokiej dostępności | Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s), RPVST+ |
| Funkcje stackowania | Obsługa VSF(Virtual Switching Framework) do czterech urządzeń w stosie przez dowolny port uplink |
| Agregacja portów | zgodna z 802.3ad LACP |
| QoS | priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek, rate-limiting, algorytm opróżniania kolejek WDRR i SP, Voice VLAN, Layer 4 prioritization, Class of Service (CoS) |
| Monitorowanie | RMON 4 grupy statistics, history, alarm, events, SFLOW |
| Oprogramowanie | Aktualizacje dostępne na stronie producenta |
| Pozostałe funkcje | LLDP,LLDP-MED, dual flash images, obsługa ramek typu Jumbo, DHCP snooping, DHCP Server, BPDU Guard, BPDU Protection, izolacja portów, wsparcie dla IPv4 i Ipv6, Tunneled node dla ruchu z AP, Zero Touch Provisioning, wsparcie dla VRRP, obsługa GVRP and MVRP |
| Obudowa | Umożliwiająca instalację w szafie 19". Wysokość max. 1U. |
| Moc pobierana maksymalna | 450W, zasilacz z certyfikatem 80 PLUS Silver |
| Zasilanie | 200 - 240 VAC |
| Środowisko pracy | 0°C do 45°C |
| Wyposażenie (dostarczone w komplecie przełącznikiem) | Wyposażenie do podłączenia dostarczonego niniejszego przełącznika PoE+ do istniejącego przełącznika 48 x 100/1000 BaseT + 4SFP (posiadanego przez Zamawiającego), który w ramach realizacji przedmiotu zamówienia Wykonawca przeniesie, zainstaluje, uruchomi i skonfiguruje w budynku Urzędu Miejskiego przy Placu Wolności 1, interfejsem o przepływności Ethernet 1Gbit/s z wykorzystaniem portów SFP (do połączenia przełączników nie dopuszcza się wykorzystywania portów 100BaseTX/1000BaseT) |
| Gwarancja | Dożywotnia (tak długo jak Zamawiający posiada produkt) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |

|  |  |  |
| --- | --- | --- |
| 1. **System analizy ruchu sieciowego – 1 szt.** | | |
| **Nazwa składnika/parametru technicznego sprzętu** | | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |
| Zakres dostawy i wdrożenia | Funkcjonalności | Zamawiający wymaga dostawy systemu analizy ruchu sieciowego obejmującego co najmniej moduły funkcjonalne:   * Zarządzania infrastrukturą IT: * Skanera sieci IP wykrywającego urządzenia podpięte do sieci. * Modułu raportów umożliwiającego tworzenie własnych wzorów raportów i wysyłania raportów zgodnie z zadanym harmonogramem. * Zdalnej instalacji programów. * Monitorowania wydajności urządzeń i ruchu sieciowego. * Komunikatora rozmów indywidualnych i grupowych pomiędzy administratorem a pracownikiem. * HelpDesk. * Skanowania środowisk wirtualnych. * Ochrony i przeciwdziałania wyciekom informacji DLP. * Gromadzenie, analizy i raportowania informacji z ruchu sieciowego. |
| Rodzaj rozwiązania | Zamawiający dopuszcza dostarczenie rozwiązania w postaci:   * komercyjnej platformy sprzętowej wraz z wewnętrznym oprogramowaniem systemowym, realizującej wszystkie wymagane funkcjonalności lub * wdrożenia rozwiązania programowego obejmującego moduły realizujące ww. funkcjonalności, przy czym Zamawiający dopuszcza instalację systemu na dodatkowych maszynach wirtualnych na dostarczanym systemie serwerowym lub dostarczenie dedykowanej platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.   W każdym przypadku, jeżeli instalacja i wdrożenie systemu analizy ruchu sieciowego wymaga dodatkowych licencji (np. na systemy operacyjne, bazodanowe, wirtualizatory, oprogramowanie instalowane na komputerach użytkowników końcowych, dostęp do konsoli administracyjnych, itp.) wykonawca zobowiązany jest dostarczyć licencje w wymaganym zakresie. |
| Licencjonowanie | Dostarczony system analizatora ruchu sieciowego zapewniać:   * Licencja wieczysta na użytkowanie 1 urządzenia centralnego lub 1 serwera systemu, * Licencję wieczystą na co najmniej 100 agentów oprogramowania instalowanego na komputerach użytkowników końcowych. * Licencję wieczystą na co najmniej 5 jednoczesnych dostępów do konsoli administracyjnej. * Licencje wieczyste skanowania maszyn wirtualnych obejmujące co najmniej 3 serwery wirtualizacji i co najmniej 10 maszyn wirtualnych. * Wsparcie techniczne przez okres co najmniej 4 lat (**jednak nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty**) obejmujące aktualizacje systemu i baz danych, dostęp do internetowej bazy wiedzy oraz wsparcie telefoniczne lub mailowe. * Dostarczenie niezbędnych licencji do systemów operacyjnych, bazodanowych, wirtualizatorów w przypadku rozwiązania programowego. |
| Zakres wdrożenia | * Dostawa rozwiązania, instalacja/wdrożenie i konfiguracja. * Profilowanie systemu. * Zdalne szkolenie administracyjne – dla min. 2 administratorów. * Co najmniej 3 zdalne sesje szkoleniowe w zakresie wybranych funkcjonalności systemu – do wykorzystania w terminie 3 miesięcy od zakończenia instalacji. |
| Architektura systemu | Elementy systemu | * Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. * Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych). * Urządzenie centralne lub serwer – odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami. * Baza danych pracująca na urządzeniu centralnym lub w przypadku wdrożenia programowego na silniku SQL w wersji dobranej w zależności od wymagań instalowanego systemu. |
| Wymagania funkcjonalne | * Wszystkie komponenty systemu muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerami aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją. * System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy. * Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI. * Agent musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi. * Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej. * Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa). * System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków. * Agent musi mieć definiowalny priorytet pracy (ABOVE\_NORMAL, NORMAL, BELOW\_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów. * Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta. * System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem. * System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów. * System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania. |
| Wymagania systemowe | * Konsola administracyjna musi działać na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera). * Agent musi działać na systemach 32 i 64 bitowych: Windows 2003 Server, Windows 2008 Server, Windows 2012 Server, Windows 16 Server, Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 10, MacOS 10.7,MacOS 10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. * Urządzenie centralne wyposażone w wewnętrzne oprogramowanie systemowe * W przypadku wdrożenia programowego: * Serwer musi działać na systemach 32 i 64 bitowych: Windows 2000, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows 2012 Server, Windows 2016 Server, Windows XP SP3, Windows Vista, Windows 7, Windows 8. * Serwer www musi być oparty o platformę: MS Windows 64-bit (Windows XP SP3, Windows Server 2003 lub nowsze) oraz Java 7 (JRE lub JDK), Apache Tomcat 7. * Baza danych musi działać na silniku SQL. * Jeśli architektura / wymagania systemu wymagają licencji typu CAL dla każdego komputera z zainstalowanym agentem należy dostarczyć wraz z systemem odpowiednią liczbę licencji CAL. * System musi mieć możliwość pracy w środowisku wirtualnym na dostarczonych serwerach. |
| Interfejsy | * System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. * Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID. * System musi umożliwiać import użytkowników z zewnętrznego pliku CSV. * System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane. * System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS. |
| Funkcjonalności systemu zarządzania infrastrukturą IT | Agent | * System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP). * Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość * Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił. * Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta. * Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania. |
| Konsola administracyjna | * Konsola musi być w pełni polskojęzyczna. * Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie). * Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi. * Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika. * Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń) * Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie). * System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność). * Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku. * System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji. * Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu. * Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko). * Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera. * Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL). * Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell) * Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta. |
| Zarządzanie licencjami | * System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów). * System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej. * Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania. * System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania”, które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe” – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe” - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone” – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze. * System umożliwia zdefiniowanie listy aplikacji zabronionych. * System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu). * System musi umożliwiać zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii. * System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji). * System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe. * System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware. * System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji. * System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji. * System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi. * System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki). * System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł. * System prezentuje datę instalacji oprogramowania. * System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium. * System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych). * System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu). * System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia. * System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności. * System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach. * System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach. * System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej. * System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej. |
| Wzorce aplikacji i pakietów | * System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,5 tys. wzorców aplikacji, 1,3 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania. * System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja. * System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania. * System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania. * Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów. * System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu. * System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.). |
| Inwentaryzacja sprzętu komputerowego | * System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem). * System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language. * System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu). * System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania. * System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru. * System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu). * System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART). * System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku. * System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane). * System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu. * System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent). * System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne. * System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów. * System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik) * System umożliwia dodawanie notatek do każdej pozycji sprzętu. * System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części). * System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium. * System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja). |
| Inwentaryzacja urządzeń podłączanych do komputera | * System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp. * System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika. * System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika). |
| Identyfikacja środowisk wirtualizacji | * System musi być wyposażony w skaner środowisk wirtualizacji Hyper-V oraz VMware. * Skaner środowisk wirtualizacji musi być w pełni programowalny, musi obsługiwać wiele środowisk wirtualizacji oraz dowolną ilość atrybutów logowania (login, hasło). * Skaner środowisk wirtualizacji musi być wyposażony w programowalny harmonogram skanowania. |
| Inwentaryzacja urządzeń innych niż komputery | * System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp. * System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNTP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). * Skaner SNTP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port. * System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na zweryfikowanie czy znalezione skanerem komputery posiadają agenta a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta. * System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych. * System musi monitorować zmiany ewidencyjne i ruchy sprzętu. * System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji. * System musi mieć możliwość przypominania o upływającym terminie gwarancji. * System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu. * System udostępnia informację o wartości wprowadzonego sprzętu. * System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość. * System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy. * System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje). |
| Ochrona danych | * System automatycznie tworzy bazę danych podpinanych do komputerów urządzeń USB. * System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.) * System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie. * System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB. * System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplekser USB). * System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły. |
| Zdalna administracja komputerami | * System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika. * System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro. * System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji. * System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6). * System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch). * System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania. * Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego. * Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status). * System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. |
| Automatyzacja | * System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące. * Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności. * System musi mieć możliwość definiowania czynności wykonywanych automatycznie. * System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów). * System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji, * System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.). * System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako) * System musi umożliwiać tworzenie zadań cyklicznych dla komputerów. * Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania. * System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie. |
| Zarządzanie magazynem IT | * System musi umożliwiać obsługę magazynu IT. * System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach. * System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI. * System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło). * System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach. * System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie. |
| Repozytorium | * Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu. * Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje. |
| Kody kreskowe | * System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych. * System wspiera parametryzację kodu w zakresie wielkości graficznej kodu. * System pozwala w każdym momencie na zmianę typu i atrybutów kodu. * System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu. * Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów. * System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail. * Obsługa kodów kreskowych nie może wymagać instalacji czcionek. * Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne. * System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów. |
| Edukacja pracowników | * System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów. * System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”. * Formatowanie treści musi być zgodne z HTML. * System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych). * System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców. * Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości. * Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania. * System musi posiadać zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości. * System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników. * System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem). * System musi posiadać możliwość eksportu / importu treści. |
| Monitorowanie wydruków | * System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa). * Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor. * System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru. * System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących. * System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy. * System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników. |
| Monitorowanie stron www | * System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej. * Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek. * Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https). * Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony. |
| Monitorowanie dziennika zdarzeń | * System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów. * Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system. * System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia. * Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia. |
| Monitorowanie pracy komputerów | * System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym. * System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego. * System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie |
| Monitorowanie sesji zdalnych połączeń | * System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze. * Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia. |
| Raportowanie i eksport danych | * Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp. * System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika). * System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów. * Generowanie raportu musi odbywać się po stronie serwera a nie klienta. * System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków). * System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt). * System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF. * System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu). * System musi posiadać co najmniej 100 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych. |
| Funkcjonalności systemu zarządzania bezpieczeństwem i ochrony danych DLP | Wymagania podstawowe | * System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących. * System musi być zgodny z wytycznymi Krajowych Ram Interoperacyjności. * System musi prowadzić szczegółową informację o zarządzanych komputerach, w sposób automatyczny (zgodnie z ustalonym harmonogramem) je inwentaryzuje. * System musi udostępniac podstawowe dane inwentaryzacyjne komputerów, m.in.: Procesor, BIOS, Pamięć, Dyski twarde, SMART, Sieć, Pliki, Czas pracy, Zdarzenia. * System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami. * System musi posiadać wysoką wydajność zapewnioną przez rozproszone i wydajne przetwarzanie danych na serwerze głównym oraz stacjach roboczych. * System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią). * System musi na bieżąco monitorować zmianę położenia danych zapobiegając ich zagubieniu /zdublowaniu /udostępnieniu za pośrednictwem dowolnych kanałów. * System musi być wyposażony w mechanizm tworzenia reguł ochrony (DLP) w oparciu o zdefiniowane polityki, obiekty docelowe, nazwy użytkowników, datę ważności polityki. * Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych. * System musi posiadać funkcjonalności monitorowania działania danej polityki, blokowanie polityki (wykonywania zdefiniowanych akcji), powiadamianie o incydencie oraz pełnego logowania zdarzeń dotyczących polityki. * Monitorowanie i ochrona danych. |
| Polityki ochrony danych | * SCHEMATY OPROGRAMOWANIA – polityka umożliwiająca zdefiniowanie schematu, na którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. * FINGERPRINT – polityka umożliwiająca oznaczanie określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami. * PRINTSCREEN – polityka umożliwiająca kontrolowanie wykonywania przez użytkowników operacji zrzutu ekranu. * SCREEN MONITORING - polityka umożliwiająca bieżący podgląd na pulpit komputera. * WORKING TIME - polityka umożliwiająca powiadamianie o przekroczeniu dozwolonego czasu pracy komputera. * PROCESS - polityka umożliwiająca podjęcie działania w momencie uruchomienia określonego procesu. * REMOVABLE DEVICE - polityka umożliwiająca monitorowanie określonych typów urządzeń przenośnych. * FILE MOVE COPY - polityka umożliwiająca na monitorowanie i blokowanie operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach. * WEB - polityka umożliwiająca zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www. * SPLASH SCREEN - polityka umożliwiająca wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne i posiadać funkcjonalność: utwórz tabelę, załącz obraz, wstaw link. * EMAIL - polityka umożliwiająca monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. * CLOUD STORAGE - polityka umożliwiająca monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą. * DEVICE - polityka umożliwiająca blokowanie lub zezwalanie działania określonym typom urządzeń dostępnych w menedżerze urządzeń. * CLIPBOARD - polityka umożliwiająca podjęcie stosownych działań w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka. Musi umożliwiać kontrolę nie tylko nad całym plikiem, ale również jego zawartością. * WLAN – polityka umożliwiająca blokowanie sieci ze względu na typ i maskę. Musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych. * E-LEARNING - polityka umożliwiająca regularne szkolenie pracowników zapewniając elektroniczną listę obecności na szkoleniach e-learningowych. Wymagana jest możliwość zdefiniowania dowolnej ilości polityk (np. kompletów szkoleniowych z zakresu bezpieczeństwa) oraz wysyłanie ich do użytkowników zgodnie ze zdefiniowanym harmonogramem. |
| Obiekty docelowe reguł definiowalne za pomocą parametrów | * Nazwa komputera * Adres IP * Unikatowy identyfikator agenta * Status podłączenia do systemu (on-line/off-line) * Zainstalowany system operacyjny * Nazwę zalogowanego użytkownika * Model komputera * Producent komputera * Dostawca komputera * Budżet, z którego zakupiony został komputer * Obecność technologii antykradzieżowej Intel® Anti-Theft * Strukturę organizacyjną |
| Znaczniki (ang. fingerprint) i użycie ich do znakowanie danych | * Możliwość samodzielnego zdefiniowania dowolnej ilości znaczników. * Znacznik nie może naruszać struktury pliku, w szczególności sygnatury podpisu cyfrowego, wielkości pliku i musi być niewidoczny dla użytkownika. * Możliwość automatycznego oznaczenia dowolnego typu pliku dowolną ilością znaczników. * Możliwość usuwania nałożonych wcześniej znaczników. * Możliwość definiowania konkretnych lokalizacji, w których pliki mają zostać oznakowane. * Możliwość wykluczenia konkretnych lokalizacji z procesu znakowania. * Możliwość definiowania maski plików do oznakowania z wykorzystaniem znaków wieloznacznych. * Możliwość wykluczenia konkretnych masek plików z procesu znakowania z wykorzystaniem znaków wieloznacznych. * Możliwość szybkiego podglądu zdefiniowanych lokalizacji oraz masek plików oznaczonych. * Automatyczne wykrywanie zdublowanych plików z wybranym znacznikiem. * Logowanie wszystkich zdarzeń związanych z nakładaniem/zdejmowaniem znacznika lub też odnalezieniem oznakowanych plików. |
| Zrzuty ekranu | * Obsługa wielu ekranów (wiele monitorów podłączonych do jednego komputera). * Obsługa pulpitów wirtualnych (logiczny rozmiar pulpitu jest większy niż fizyczny rozmiar ekranu). * Możliwość monitorowania/zablokowania wykonania zrzutu ekranu przez użytkownika za pomocą klawiatury. * Szczegółowe logowanie próby wykonania zrzutu ekranu, zawierające m. in. graficzną reprezentację ekranu w momencie zajścia incydentu. |
| Monitoring wizualny | * Obsługa wielu ekranów (wiele monitorów podłączonych do jednego komputera). * Obsługa pulpitów wirtualnych (logiczny rozmiar pulpitu jest większy niż fizyczny rozmiar ekranu). * Możliwość śledzenia zawartości ekranu użytkowników poprzez bieżący dostęp do chronologicznego zapisu zrzutów ekranu. * Częstotliwość pozyskiwania automatycznego zrzutu ekranu konfigurowana przez administratora. * Mechanizm zabezpieczający przed przepełnieniem bazy danych zbyt dużą ilością zrzutów ekranu. * Czytelny podgląd obrazów (zrzutów ekranowych) za pomocą widoku siatki. |
| Monitorowanie czasu pracy | * Możliwość zdefiniowania dowolnej ilości reguł dotyczących czasu pracy komputera. * Możliwość zdefiniowania zalecanego czasu pracy dla każdego komputera. * Czas pracy w każdym dniu tygodnia może być zdefiniowany inaczej. * Możliwość automatycznego dołączenia bieżącego zrzutu ekranu to każdego incydentu związanego z przekroczeniem zalecanego czasu pracy urządzenia. |
| Uruchamiane procesy i aplikacje | * Możliwość zdefiniowania dowolnej ilości reguł dotyczących uruchamiania aplikacji. * Możliwość zdefiniowania procesów, które będą monitorowane/blokowane przez system za pomocą maski zawierającej znaki wieloznaczne (\* oraz ? zastępujące odpowiednio dowolny ciąg znaków oraz znak pojedynczy). * Możliwość dołączenia bieżącego zrzutu ekranu to każdego incydentu związanego z próbą uruchomienia monitorowanego procesu. |
| Monitorowanie urządzeń przenośnych | * Możliwość tworzenia grup urządzeń przenośnych wg kryteriów: identyfikator sprzętowy. * Automatyczne inwentaryzowanie (identyfikator sprzętowy, nazwa) urządzeń przenośnych podłączanych do komputerów użytkowników. * Możliwość ręcznego dodawania urządzeń przenośnych. * Możliwość wykluczania grup urządzeń przenośnych z monitorowania (tzw. biała lista). * Możliwość definiowania dni tygodnia oraz zakresu godzin, w których ma być aktywne monitorowanie urządzeń przenośnych. * Możliwość jednoczesnego odczytania wielu identyfikatorów urządzeń przenośnych za pomocą multiplikatora portów USB za pomocą wbudowanej funkcji/aplikacji. * Możliwość dołączenia bieżącego zrzutu ekranu to każdego incydentu związanego z użyciem urządzenia przenośnego. |
| Operacje w systemie plików | * Dokładne monitorowanie zdarzeń (otwarcie, usunięcie, utworzenie, zapis, zamian nazwy pliku) w całym systemie plików. * Możliwość deklarowania lokalizacji podlegających monitorowaniu (oraz lokalizacji wykluczonych z monitorowania) z użyciem znaków wieloznacznych. * Możliwość definiowania maski plików podlegających monitorowaniu (oraz wykluczonych z monitorowania) z użyciem znaków wieloznacznych. * Możliwość śledzenia każdego rodzaju operacji (usunięcie pliku, utworzenie pliku, zapis do pliku, zmiana nazwy pliku, a w szczególności otwarcie pliku). * Możliwość deklarowania procesów, których dostęp do systemu plików będzie monitorowany z użyciem znaków wieloznacznych. * Możliwość stworzenia białej listy procesów, których dostęp do systemu plików nie będzie monitorowany. * Możliwość monitorowania systemu plików w oparciu o znaczniki założone przez system. |
| Dostęp do stron WWW | * Możliwość zdefiniowania stron podlegających monitorowaniu / blokowaniu za pomocą znaków wieloznacznych. * Możliwość zdefiniowania stron wykluczonych z monitorowania / blokowania za pomocą znaków wieloznacznych. * Możliwość blokowania stron w oparciu o protokół nieszyfrowany (http) oraz szyfrowany (https). * Kompatybilność z korporacyjnym (firmowym) serwerem Proxy. * Wsparcie dla przeglądarek IE, Edge, Firefox, Opera, Chrome oraz innych wspierających komunikację przez serwery Proxy. |
| Kanał poczty elektronicznej e‑mail | * Możliwość zdefiniowania maski plików, które będą podlegały monitorowaniu/blokowaniu w zakresie ich użycia (wysyłania) w programach pocztowych za pomocą znaków wieloznacznych. * Możliwość definiowania masek plików wykluczonych z monitorowania ich użycia w programach pocztowych za pomocą znaków wieloznacznych. * Wsparcie dla rozwiązań poczty chmurowej (np. Microsoft OWA). |
| Ochrona dostępu do rozwiązań chmurowych | * Możliwość zdefiniowania maski plików, które będą podlegały monitorowaniu/blokowaniu w zakresie ich transportu z lub do rozwiązania chmurowego. * Możliwość zdefiniowania masek plików wykluczonych z monitorowania w zakresie ich transportu z lub do rozwiązania chmurowego. * Wsparcie (monitorowanie/blokowanie) dla następujących rozwiązań chmurowych: BitTorrent Sync, Box, Copy, Cubby, Dropbox, Google Drive, Knowhow Cloud, Mediafire, Mega, Microsoft OneDrive, Mozy, Spideroak, STRATO HiDrive, Tresorit. |
| Zabezpieczenia urządzeń | * Możliwość blokowania grup urządzeń wg nazwy. * Możliwość blokowania grup urządzeń wg typu: Stacje dysków CD-ROM/DVD, Czujniki, Czytniki kart inteligentnych, Drukarki, GPS, Imaging Devices, Karty graficzne, Karty sieciowe, Klawiatury, Kontrolery dźwięku, wideo i gier, Kontrolery IDE ATA/ATAPI, Kontrolery IEEE 1394 Host Bus, Kontrolery magazynu, Kontrolery uniwersalnej magistrali szeregowej, Kopie w tle woluminów magazynu, Modemy, Mysz i inne urządzenia wskazujące, Napędy dyskietek, Napędy taśmowe, PCMCIA adaptery, Porty (COM i LPT), Przenośne urządzenia z systemem Windows (WPD), Software devices, Stacje dysków, Urządzenia akumulatorowe, Urządzenia biometryczne, Urządzenia Bluetooth, Urządzenia interfejsu HID, Urządzenia IrDA, Urządzenia wielofunkcyjne , Urządzenia zgodne ze standardem IEEE 1284.4, Urządzenie USB, Wieloportowe karty szeregowe, Windows CE ActiveSync USB Urządzenia, Woluminy magazynu, Zmieniarki mediów. * Możliwość odblokowania zablokowanych urządzeń. * Logowanie procesu blokowania/odblokowania urządzeń z danej grupy. * Możliwość dołączenia bieżącego zrzutu ekranu to każdego incydentu związanego z blokowaniem/odblokowaniem urządzenia. |
| Powiadomienia użytkowników | * Możliwość powiadomienia użytkownika komputera o każdym naruszeniu polityki lub incydencie związanym z wystąpieniem alertu DLP, zarówno z aktywnym blokowaniem incydentu (blokada i powiadomienie) jak i bez blokowania (tylko powiadomienie). * Konfigurowalna treść powiadomienia osobno dla każdej reguły ochrony danych. * Możliwość wykorzystania w komunikatach słów kluczowych – zmiennych systemowych (np. %UserName%, %FileName%, itp.), które w komunikacie dla użytkownika zostają automatyczne zastąpione konkretnymi danymi. * Wyświetlanie nieinwazyjnego komunikatu na bieżącym pulpicie użytkownika. |
| Powiadomienia administratorów | * Powiadomienia administratorów na pulpicie konsoli administracyjnej o wszystkich incydentach w organizacji z możliwością szybkiego przejrzenia szczegółów incydentów. * Możliwość powiadomienia administratora o każdym naruszeniu polityki lub incydencie związanym z wystąpieniem alertu DLP za pomocą poczty e-mail. * Konfigurowalna treść powiadomienia osobno dla każdej reguły DLP. * Możliwość wykorzystania w komunikatach słów kluczowych – zmiennych systemowych (np. %UserName%, %FileName%, itp.), które w ostatecznym komunikacie zostaną zastąpione konkretnymi danymi. * Obsługa szyfrowanych protokołów poczty e-mail. * Możliwość definiowania dowolnej liczby odbiorców powiadomień. * Możliwość łatwego (jednym przyciskiem) testowania konfiguracji połączenia z serwerem poczty e-mail. |
| Zarządzanie polityką bezpieczeństwa | * Możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP. * Możliwość instalacji polityk i reguł na wybranych komputerach w czasie nie dłuższym niż 60 sekund (przy założeniu, że komputer jest osiągalny w sieci lokalnej lub za NATem) w sposób przezroczysty dla użytkowników komputerów i bez konieczności jakiejkolwiek ingerencji administracyjnej na komputerach oraz bez konieczności restartu komputerów. * Instalacja polityk i reguł musi być również wykonywana dla komputerów za NATem. * Możliwość dezaktywacji danej reguły bez jej wyłączania i utraty konfiguracji. * Powiadomienie o konieczności instalacji nowej polityki DLP w przypadku jej modyfikacji w dowolnym miejscu systemu. * Możliwość definiowania obiektów, na których działać będzie dana reguła w oparciu o: nazwę komputera, adres IP, unikatowy identyfikator agenta, nazwę systemu operacyjnego, zalogowanego użytkownika, model komputera, dostępność technologii Intel® Anti-Theft, strukturę organizacyjną, producenta komputera, dostawcę komputera, budżet z jakiego komputer został zakupiony. * Nowy komputer zgłaszający się do systemu po raz pierwszy, musi automatycznie, bez dodatkowej ingerencji administratora pobrać automatycznie oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę ochrony. * Możliwość wykluczenia grupy użytkowników ze stosowania jednej lub wielu reguł ochrony DLP. * Możliwość określenia ram czasowych działania danej reguły DLP. Polityki po czasie ważności muszą być automatycznie deaktywowane. Deaktywacja musi następować zarówno na komputerach podłączonych do sieci komputerowej jak i znajdujących się poza siecią. * Możliwość dołączenia dowolnego opisu dla każdej reguły ochrony DLP. * Podgląd postępu instalacji polityk na komputerach nie wymaga ciągłego odświeżania widoku. * Procentowy wskaźnik postępu instalacji polityk wraz z listą komputerów z zainstalowaną polityką i bez zainstalowanej polityki. * Możliwość działania poszczególnych polityk ochrony DLP w oparciu o znacznik FINGERPRINT. * Monitorowanie dostępu musi odbywać się na poziomie jądra systemu Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego. * Znacznik czasowy incydentów DLP jest niezależny od ustawień lokalnego daty/czasu na komputerze użytkownika - incydenty DLP zawsze zgłaszane będą ze znacznikiem czasowym serwera DLP. |
|  |
| Integracja systemu zarządzania infrastrukturą IT z systemem zapobiegania wyciekom danych (DLP) | Wymagania podstawowe | * System ochrony DLP oraz system zarządzania infrastrukturą muszą być oparte o jednego agenta spełniającego jednocześnie rolę agenta systemu zarządzania infrastrukturą oraz agenta ochrony DLP. * Interfejs (konsola administracyjna) systemu ochrony DLP musi być w pełni zgodna z interfejsem systemu do zarządzania infrastrukturą IT, w szczególności w zakresie budowy, logiki użytkowej, zasad filtrowania/wykluczania danych, eksportu i drukowania, prezentacji danych, praw dostępu do danych oraz poszczególnych funkcjonalności tak, aby użytkownik jednego systemu bez konieczności szkoleń i korzystania z dokumentacji potrafił pracować na drugim systemie. * Zalogowanie do jednego z systemów umożliwia jednoczesne korzystanie z drugie systemu i nie wymaga ponownego logowania do systemu DLP. |
| Bezpieczeństwo | Wymagania podstawowe | * System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej. * Siła hasła użytkownika musi być definiowalna w systemie w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków). * Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport. * System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów. * System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera. * System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii. * System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych. * W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy). * System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów. * System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji. |
| Uwierzytelnianie do systemu | * Z wykorzystaniem imiennego konta użytkownika i hasła; * Z wykorzystaniem imiennego konta administratorów aplikacji i hasła; * Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej; * Za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory. |
| Logi systemowe | * Pełne logowanie błędów w celu weryfikowania nieprawidłowości. * Przechowywanie logów systemowych. * Przechowywanie logów bezpieczeństwa. * Przechowywanie logów aktywności użytkowników i administratorów. * Pobieranie logów z agentów z poziomu konsoli administracyjnej. * Możliwość eksportu logów. * Definiowanie maksymalnego czasu przechowywania plików log. |
| Moduł gromadzenia, analizy i raportowania informacji z ruchu sieciowego | Wymagania podstawowe | * Zcentralizowane gromadzenie i przetwarzanie logów i informacji o zdarzeniach. * Analiza i przeszukiwanie zebranych logów w celu znalezienia i przeanalizowania informacji o istotnych zdarzeniach. * Wizualizacja danych. * Raportowanie. * Alarmowania i wymuszanie działań na podstawie wykrycia określonych zdarzeń, wyjątków, pogorszenia wydajności, itp. |
| Gromadzenie logów | * Możliwość zapisu logów z różnych źródeł, w tym urządzeń pracujących w sieci, komputerów, serwerów, UTM, aplikacji, systemów bazodanowych, itp. * Wbudowany mechanizm retencji. * Indeksowanie danych Syslog, plików płaskich oraz danych biznesowych. * Praca w środowisku rozproszonym. * Praca w modelu klastrowym. |
| Analiza | * Przegląd zapisanych logów. * Przeszukiwanie zbiorów logów na podstawie zadanych kryteriów, np. składni, rodzaju zdarzenia. * Definiowanie kryteriów wyszukiwania przez użytkownika. * Tworzenie filtrów. * Tworzenie zaawansowanych filtrów i korelacji zdarzeń. |
| Przegląd i wizualizacja | * Możliwość definiowania i dodawania widoków i układów ekranów. * Możliwość prezentacji danych w formie tabelarycznej, wykresów, diagramów, definiowanych widoków. * Możliwość prezentacji danych aktualnych oraz w ujęciu czasowym. * Prezentacja danych wg zadanych kryteriów. |
| Raportowanie i udostępnianie danych | * Eksport danych exportu dużych porcji danych do formatu CSV. * Eksport danych wg zadanych kryteriów. |
| Reakcja na zdarzenia | * Definiowanie wyzwalaczy. * Tworzenie reguł alarmowych definiowanych przez użytkownika na podstawie braku danych, wzrostu ilości logowanych danych, zdefiniowanych kryteriów analizowania danych. * Wysyłanie powiadomień w postaci komunikatów lub wiadomości mail przypadku wykrycia określonych zdarzeń. * Wykonywanie zadanych akcji na podstawie wykrycia określonych zdarzeń. |
| Bezpieczeństwo | * Mechanizm konfiguracji użytkowników, ról i uprawnień poziomu GUI. * Podział widoczności danych do wskazanych indeksów dla wybranych grup * Użytkowników. * Integracja z istniejącym katalogiem użytkowników LDAP. * Zapis historii działań i zmian dokonywanych w systemie przez użytkowników i administratorów (logi wewnętrzne). * Audyt logów wewnętrznych. |
| Integracja | Zakres integracji z istniejącymi systemami | W ramach wdrożenia systemu analizy ruchu sieciowego należy przygotować wdrażany Moduł gromadzenia, analizy i raportowania informacji z ruchu sieciowego do integracji z posiadanym przez Zamawiającego systemem do nadzoru urządzeń sieciowych typu MNS oraz zbierania logów z posiadanych przez Zamawiającego wszystkich urządzeń sieciowych, w tym urządzeń z sieci LAN, urządzeń pracujących w sieci szerokopasmowej gminy Olecko, urządzeń systemu monitoringu miejskiego, z wykorzystaniem protokołów:  - Syslog  - SNMP  W ramach wdrożenia należy przekazać wytyczne nt. sposobu konfiguracji posiadanych przez niego urządzeń do udostępniania logów do wdrażanego Moduł gromadzenia, analizy i raportowania informacji z ruchu sieciowego. |
| Wsparcie i pomoc | Wymagania podstawowe | * System musi posiadać podpowiedzi dziedzinowe (porady) w obszarze licencjonowania. |
| Dokumentacja | * Wbudowana dokumentacja pomocy użytkownika w języku polskim lub angielskim, * Dostępność filmów instruktażowych w języku polskim obejmujących instrukcje konfiguracji głównych funkcjonalności systemu. |
| Pomoc techniczna | * Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. |

|  |  |
| --- | --- |
| 1. **Serwer – 2 sztuki pracujące w trybie HA** | |
| **Nazwa składnika/parametru technicznego sprzętu** | **Minimalne wymagania w zakresie składników i parametrów technicznych pojedynczego serwera** |
| **Procesor** | Zainstalowane dwa procesory 10-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem.  Zaoferowany serwer z dwoma procesorami musi umożliwiać osiągnięcie wyniku min. 905 punktów w teście SPECint\_rate\_base2006. Wynik testu musi być publikowany na stronie [www.spec.org](http://www.spec.org) |
| **Pamięć operacyjna** | Zainstalowane min. 128GB pamięci RAM DDR4.  Na płycie głównej powinny znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.  Zabezpieczenia pamięci: Advanced ECC oraz Online Spare. |
| **Pamięć masowa** | Zainstalowane min. 2 dyski 240GB Read Intensive SSD SATA 6G.  Możliwość instalacji do min. 8 dysków typu HotSwap SATA, SAS, SSD 2.5” oraz 2 dysków M.2. |
| **Interfejsy sieciowe** | Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT z funkcją Wake-On-LAN, RJ45, niezajmujące slotów PCI-E.  Zainstalowane:  - dwie dwuportowe karty sieciowe 10Gb Ethernet  - dwuportowa karty FiberChannel 16Gb/s z wkładkami optycznymi, przy czym każdy port powinien posiadać niezależny procesor i pamięć (dopuszcza się zastosowanie dwóch niezależnych kart jednoportowych FiberChannel 16Gb/s). |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji w szafie rack 19”, w komplecie wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie oraz organizerem na kable montowanym z tyłu obudowy. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Sloty PCI Express** | Serwer z co najmniej 3 slotami PCI-Express Generacji 3:   * co najmniej 2 sloty PCI-Express Generacji 3 działające z prędkością x16 (bus width), w tym dwa jeden pełnej długości i wysokości. * co najmniej 1 slot PCI-Express Generacji 3 działający z prędkością x8 (bus width) pełnej wysokości. |
| **Zasilanie i chłodzenie** | Zasilacze typu Platinum - minimum 2szt., redundantne, typu hot-plug o mocy maksymalnie 800W każdy.  Zestaw redundantnych wentylatorów typu hot-plug. |
| **Kontroler dyskowy** | Kontroler macierzowy SAS 12Gb z min. 2GB cache, z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę do 16 napędów dyskowych SAS oraz obsługujący poziomy:  RAID 0/1/1+0/5/5+0/6/6+0.  Możliwość rozbudowy pamięci cache do 4GB poprzez rozbudowę kontrolera lub wymianę kontrolera. |
| **Grafika** | Zintegrowana z płytą główną |
| **Interfejsy i porty** | 5 x USB 3.0 (w tym dwa wewnętrzne).  1x VGA  Wewnętrzny slot na kartę microSD/SD.  Display Port dostępny z przodu serwera.  Port USB dedykowany do zarządzania z przodu obudowy.  Port szeregowy.  Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń. |
| **Gwarancja** | Co najmniej 4 lata gwarancji producenta (**jednak nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty**) realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 9x5 (od poniedziałku do piątku, w godzinach 8 -17) poprzez ogólnopolską linię telefoniczną lub system zgłoszeń producenta.  Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. |
| **Zarządzanie i obsługa techniczna** | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS) . Funkcjonalność przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD.  Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, minimum 4GB, w tym minimum 1GB dostępny dla użytkownika serwera.  Karta zarządzania zdalnego, udostepniająca wbudowane narzędzie wspomagające instalację systemów operacyjnych oraz konfigurację serwera. Narzędzie dostępne z poziomu BIOS poprzez interfejs graficzny (GUI), udostępniające minimum następujące funkcjonalności:   * wspomaganą instalację systemu operacyjnego – wybór najlepszych sterowników i firmware, * diagnostykę wszystkich elementów sprzętowych serwera, * konfigurację kontrolera macierzowego i dysków poprzez GUI, * ustawienia parametrów BIOS.   Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.  Serwer musi posiadać deklaracja CE. |
| **Obsługa systemów operacyjnych i systemów wirtualizacyjnych** | Microsoft Windows Server min. w wersji 2012R2 i 2016  Ubuntu  Red Hat Enterprise Linux (RHEL)  SUSE Linux Enterprise Server (SLES)  VMware  Citrix XenServer  Oracle Linux |

|  |  |  |
| --- | --- | --- |
| 1. **Serwerowy system operacyjny – 1 komplet** | | |
| **Nazwa funkcjonalności / parametru technicznego** | **Minimalne wymagania w zakresie funkcjonalności / parametrów technicznych** | |
| **Architektura systemu** | System przeznaczony do obsługi dwóch serwerów dostarczonych w ramach realizacji przedmiotu zamówienia, pracujących w trybie wysokiej dostępności HA (High Availability) | |
| **Licencjonowanie** | W ramach realizacji przedmiotu zamówienia wymagane jest dostarczenie licencji z prawem wieczystego użytkowania zapewniających co najmniej:   * uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i co najmniej **czterech** wirtualnych środowisk serwerowego systemu operacyjnego dla pełnej liczby rdzeni w dostarczonych 2 serwerach fizycznych wraz z obsługą funkcjonalności HA, * uruchomienia dodatkowych środowisk serwerowego systemu operacyjnego lub innych systemów operacyjnych wraz z obsługą funkcjonalności HA, w ilości wymaganej do uruchomienia wdrażanego zintegrowanego systemu informatycznego, * podłączenie do systemu co najmniej 53 użytkowników wewnętrznych pracujących w sieci wewnętrznej urzędu i jednostek podległych, w których wdrożony zostanie zintegrowany system informatyczny, * dostęp do korzystania e-usług wdrożonych w ramach projektu przez nieograniczoną liczbę użytkowników zewnętrznych .   Dostarczone licencje powinny zapewniać funkcjonowanie wdrożonego zintegrowanego systemu informatycznego i korzystania z e-usług na dostarczonej platformie sprzętowej, tj. dwóch serwerach pracujących w trybie klastra wysokiej dostępności HA (High Availability). | |
| **Funkcjonalności** | 1. | Licencja na serwerowy system operacyjny musi obejmować wszystkie rdzenie każdego procesora fizycznego na każdym serwerze. |
| 2. | Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. |
| 3. | Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. |
| 4. | Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. |
| 5. | Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |
| 6. | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |
| 7. | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |
| 8. | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
| 9. | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. |
| 10. | Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c. umożliwiają kompresję w locie; dla wybranych plików i/lub folderów,  d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
| 11. | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |
| 12. | Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |
| 13. | Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET |
| 14. | Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów |
| 15. | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych |
| 16. | Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych |
| 17. | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe |
| 18. | Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji |
| 19. | Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), |
| 20. | Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. |
| 21. | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
| 22. | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
| 23. | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
| 24. | Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). |
| 25. | Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |
| 26. | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. lub wyższy  c. Zdalna dystrybucja oprogramowania na stacje robocze.  d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  i. Dystrybucję certyfikatów poprzez http  ii. Konsolidację CA dla wielu lasów domeny,  iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. Szyfrowanie plików i folderów.  g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.  i. Serwis udostępniania stron WWW.  j. Wsparcie dla protokołu IP w wersji 6 (IPv6),  k. Wsparcie dla algorytmów Suite B (RFC 4869),  l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  iii. Obsługi 4-KB sektorów dysków  iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) |
| 27. | Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
| 28. | Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). |
| 29. | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |
| 30. | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
| 31. | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |

|  |  |
| --- | --- |
| 1. **Macierz dyskowa – 1 sztuka** | |
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19”. Wysokość maksymalnie 2U wraz z kompletem elementów do montażu w szafie Rack z możliwością instalacji minimum 12 dysków 3.5” i 2.5” typu Hot-Plug. |
| **Możliwość rozbudowy** | Macierz musi umożliwiać rozbudowę przez dodanie kolejnych dysków/półek dyskowych (bez wymiany kontrolerów macierzy), do co najmniej 190 dysków twardych. |
| **Kontrolery** | Minimum dwa kontrolery macierzowe pracujące w trybie active-active, posiadające łącznie minimum osiem portów FC minimum 16 Gb/s wraz z zainstalowanymi 4 wkładkami SFP (po 2 do każdego kontrolera) do podłączenia przełącznika Fiber Channel.  Kontrolery powinny posiadać możliwość rozbudowy o dodatkowe 4 porty iSCSI 10GbE lub FC 16 Gb/s oraz udostępniać jednocześnie dane blokowe w sieci FC z możliwością pracy z protokołem iSCSI. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.  Każdy kontroler macierzowy powinien być wyposażony w minimum 6 GB pamięci cache, 12 GB sumarycznie w macierzy. Pamięć cache kontrolerów musi być zbudowana w oparciu o wydajną pamięć typu RAM.  Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| **Pamięć cache** | Co najmniej 1,6TB pamięci cache w dyskach SSD, realizującej funkcje cache dla odczytów oraz tiering w celu zwiększenia wydajności macierzy. Zamawiający dopuszcza instalację dysków cache SSD w maksymalnie 2 kieszeniach Hot-Plug, pod warunkiem, że zaoferowane rozwiązanie umożliwia poprawną pracę takiej konfiguracji i spełniaja wszystkie wymagania.  Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD. |
| **Dyski twarde** | Macierz musi obsługiwać dyski SSD, SAS i NL SAS oraz umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie macierzy.  Zainstalowane dyski :  - co najmniej 4 dyski o pojemności minimum 4TB w technologii 12G SAS i prędkości obrotowej min. 7.2k obr/min., typu Hot-Plug. |
| **Sposób zabezpieczenia danych** | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5 lub RAID50 oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping).  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. |
| **Zarządzanie grupami dyskowymi oraz dyskami logicznymi** | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. |
| **Thin Provisioning** | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Wewnętrzne kopie migawkowe** | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Macierz musi obsługiwać minimum 512 kopii.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Wewnętrzne kopie pełne** | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Migracja danych w obrębie macierzy** | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 2 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Zdalna replikacja danych** | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Podłączanie zewnętrznych systemów operacyjnych** | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| **Zarządzanie** | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego, w tym SSH. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| **Oprogramowanie** | Wraz z macierzą należy dostarczyć oprogramowanie i wymagane licencje (dla całej pojemności urządzenia) zapewniające:   * funkcje cache dla odczytów oraz tiering z wykorzystaniem pamięci flash w celu zwiększenia wydajności macierzy, * Thin Provisioning, * wewnętrzne kopie migawkowe (minimum 512 kopii), * wewnętrzne kopie pełne, * migrację danych w obrębie macierzy, * zdalną replikacja danych. |
| **Bezpieczeństwo** | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. |
| **Dodatkowe wymagania** | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. |
| **Warunki gwarancji** | Co najmniej 4 lata gwarancji producenta (**nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty**) realizowanej w miejscu instalacji sprzętu, z gwarantowanym czasem reakcji do 4 godzin od momentu wysłania zgłoszenia do serwisu, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta lub system zgłoszeń producenta.  Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. |
| **Dokumentacja** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |
| **Certyfikaty** | Macierz wyprodukowana zgodnie z normą ISO 9001:2008 oraz 14001 |

|  |  |
| --- | --- |
| 1. **Przełącznik Fibre Channel – 1 sztuka** | |
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| **Porty i wkładki SFP** | Switch FC w architekturze Non-Blocking z aktywnymi 12 portami 16Gb FC obsadzonymi 12 wkładkami SFP 16Gb SW. Możliwość rozbudowy do 24 portów aktywnych w ramach oferowanego urządzania. |
| **Wspierane prędkości** | Wsparcie dla prędkości 4, 8, 16 Gb FC |
| **Typy portów** | Wsparcie dla typów portów D\_Port (Diagnostic Port), E\_Port, EX\_Port, F\_Port, M\_Port (Mirror Port), (U\_Port) |
| **Montaż** | Zestaw montażowy do szafy Rack. Wysokość nie większa niż 1U |
| **Firmware** | Upgrade firmware typu non-disruptive |
| **Funkcjonalności** | Funkcjonalność Zoning. Możliwość budowy połączenia Trunk między przełącznikami umożliwiającą agregacji, co najmniej 4 portów. |
| **Wydajność** | Wydajność switcha 384 Gbit/set czas opóźnienia 700 ns |
| **Zarządzanie** | Zarządzanie poprzez Web oraz CLI, SSH |
| **Kompatybilność** | Zgodność z oferowaną macierzą oraz środowiskiem serwerowym |
| **Zasilanie** | Pobór mocy nie więcej niż 80W przy maksymalnym obsadzeniu portami. |
| **Wyposażenie dostarczone w komplecie przełącznikiem** | a) Kabel połączeniowe optyczne do wykonania podłączeń 4 portów Fiber Channel serwerów do przełącznika  b) Kabel połączeniowe optyczne do wykonania podłączeń 4 portów Fiber Channel macierzy (po 2 porty z każdego kontrolera) do przełącznika  c) Kable połączeniowe optyczne do wykonania podłączeń 2 portów Fiber Channel serwera (posiadanego przez Zamawiającego, zainstalowanego w oddzielnej szafie serwerowej)  d) Kable połączeniowe optyczne do wykonania podłączeń 2 portów Fiber Channel macierzy (posiadanej przez Zamawiającego, zainstalowanego w oddzielnej szafie serwerowej) |
| **Gwarancja i wsparcie serwisowe** | | Co najmniej 4 lata gwarancji producenta (**nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty**) realizowanej w miejscu instalacji sprzętu, z gwarantowanym czasem reakcji do 4 godzin od momentu wysłania zgłoszenia do serwisu, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta lub system zgłoszeń producenta.  Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta. |

|  |  |
| --- | --- |
| 1. **Stacjonarny zestaw komputerowy – 33 sztuki** | |
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| **Typ** | Komputer stacjonarny. Typu All in One, zintegrowany komputer w obudowie wraz z monitorem. W ofercie wymagane jest podanie modelu, symbolu, producenta komputera. |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| **Procesor** | Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 7990 punktów na dzień złożenia oferty  Wynik dostępny na stronie [*https://www.cpubenchmark.net/cpu\_list.php*](https://www.cpubenchmark.net/cpu_list.php) |
| **Pamięć operacyjna RAM** | Zainstalowane 8GB (1x8GB) DDR4 2400MHz  Możliwość rozbudowy do min. 32GB., wolny minimum jeden slot na dalszą rozbudowę. |
| **Parametry pamięci masowej** | Min. 2.5” 500GB HDD |
| **Wydajność grafiki** | Zintegrowana z płytą główną, ze wsparciem dla DirectX 12.1, OpenGL 4.4, Open CL 1.2 oraz dla rozdzielczości 4096x2304@60Hz.  Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1100 punktów w G3D Rating, wynik dostępny na stronie : <http://www.videocardbenchmark.net/gpu_list.php> |
| **Matryca** | Niedotykowa, antyodblaskowa matryca IPS o przekątnej min. 21,5” (plamka max. 0,25mm) umożliwiająca wyświetlenie obrazu o rozdzielczości FHD (1920x1080) przy częstotliwości odświeżania 60Hz. Jasność matrycy co najmniej 250 cd/m², kontrast co najmniej 1000:1. Kąty widzenia pion/poziom min. 176/176 stopni. |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, budowane dwa głośniki min. 2W.  Wbudowana w obudowę matrycy cyfrowa kamera o rozdzielczości co najmniej 720p, z manualnym zamknięciem obiektywu kamery.  Wbudowany mikrofon.  Wbudowana nagrywarka DVD +/-RW SLIM |
| **Obudowa** | Typ: All-in-One zintegrowana z monitorem min. 21,5”.  Zabezpieczenie antykradzieżowe: możliwość zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) lub kłódki (oczko w obudowie do założenia kłódki).  Podstawa: możliwość regulacji w zakresie:   * kąt pochylenia w pinie – regulacja min. 20 stopni (-3 / +17) * regulacja wysokości – do min 100mm * obrót lewo/prawo – w zakresie min. 45 stopni   Wymiary: maksymalna suma wymiarów (bez podstawy) – 96 cm  Waga (bez podstawy): maksymalnie 6,5 kg  Obudowa powinna posiadać co najmniej:   * 1 zewnętrzną półkę 5,25” SLIM, * 1 wewnętrzną półkę 2,5” umożliwiającą zamontowanie dysku 2,5” (HDD/SSD/SED), * 1 slot M.2 PCIe x4 dla dysku SSD.   Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta.  Obudowa musi umożliwiać wymianę 2,5” dysku twardego, napędu optycznego oraz pamięci RAM bez użycia narzędzi czy też śrub motylkowych.  Wymagany jest wbudowany fabrycznie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej:   * awarię procesora, * uszkodzenie kontrolera Video, * uszkodzenie pamięci RAM, * uszkodzenie zasilacza.   Zasilacz: mocy maksymalnie 160W i sprawność minimum 91% przy 50% obciążeniu zasilacza i 88% przy 100% obciążeniu zasilacza (80 PLUS GOLD) |
| **Zgodność z systemami operacyjnymi i standardami** | Potwierdzenie kompatybilności komputera z zaoferowanym systemem operacyjnym (wydruk ze strony internetowej) |
| **Bezpieczeństwo** | 1. BIOS powinien zapewniać:  * skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, * możliwość ustawienia hasła na dysku (drive lock), * blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio, * blokady/wyłączenia poszczególnych kart rozszerzeń/slotów PCIe/M.2, * kontroli sekwencji bootowania, * startu systemu z urządzenia USB, * funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.  1. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2). 2. Możliwość zapięcia linki typu Kensington lub kłódki do dedykowanego oczka w obudowie komputera. 3. Udostępniona bez dodatkowych opłat, pełna wersja oprogramowania, szyfrującego zawartość twardego dysku zgodnie z certyfikatem X.509 oraz algorytmem szyfrującym AES 256bit, współpracującego z wbudowaną sprzętową platformą bezpieczeństwa. 4. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:  * informacje o systemie, co najmniej:   Procesor: typ procesora, jego obecną prędkość  Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta  Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku  Napęd optyczny: model, wersja firmware, nr seryjny  Data wydania i wersja BIOS  Nr seryjny komputera   * możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera * możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej * rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii |
| **Zarządzanie** | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym, posiadająca sprzętowe wsparcie technologii wirtualizacji, wbudowany sprzętowy firewall, zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji, a także umożliwiająca:   * monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS płyty głównej; * zdalną konfigurację ustawień BIOS; * zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; * zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; * technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/); * nawiązywanie przez sprzętowy mechanizm zarządzania zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego * (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; * wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego. |
| **BIOS** | Możliwość odczytania z BIOS:   * Wersji BIOS wraz z datą wydania wersji * Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3 * Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach * Informacji o dysku twardym: model, pojemność, * Informacji o napędzie optycznym: model, * Informacji o MAC adresie karty sieciowej   Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, serial portu, portów USB (bok, tył), funkcjonalności ładowania zewnętrznych urządzeń przez port USB, wewnętrznego głośnika, funkcji TurboBoost, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.  Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora.  BIOS musi posiadać funkcję automatycznej aktualizacji przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |
| **Certyfikaty i standardy** | 1. Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) 2. Deklaracja zgodności CE (załączyć do oferty) 3. Komputer musi spełniać wymogi normy EPEAT na poziomie min GOLD   Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.epeat.net> – wymaga się wydruku ze strony internetowej |
| **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 29 dB (załączyć odpowiedni certyfikat lub deklarację producenta) |
| **Warunki gwarancji** | Co najmniej 4 lata gwarancji producenta **(nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty)** realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub system zgłoszeń producenta.  Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta. |
| **Wsparcie techniczne producenta** | Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:   * weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć), * czasu obowiązywania i typ udzielonej gwarancji.   Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera. |
| **System Operacyjny** | Zainstalowany system operacyjny PC spełniający poniższe wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   * wersja 64-bitowa, * obsługa min. 16 GB pamięci RAM, * polska wersja językowa, * graficzne środowisko pracy, instalacji i konfiguracji, * obsługa większości powszechnie używanych urządzeń peryferyjnych (urządzeń sieciowych, standardów USB, Plug & Play, Wi-Fi), * obsługa pracy w domenie, kontroli użytkowników i zarządzania zasadami grupy, * mechanizm szyfrowania dysków twardych, pojedynczych plików oraz katalogów i nośników wymiennych, * zdalny dostęp do komputera przez pulpit zdalny, * zcentralizowane zarządzanie oprogramowaniem i konfiguracją systemu w technologii polityk/zasad grup, * w ramach dostarczonej licencji dostępne bez dodatkowych opłat aktualizacje systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa), * możliwość odroczenia aktualizacji o określony przez administratora czas, * dokonywanie uaktualnień sterowników urządzeń przez Internet – przez witrynę producenta systemu, * wbudowana zapora internetowa (firewall), dla ochrony połączeń internetowych, * wirtualizacja systemów klienckich jak i serwerowych (możliwość uruchomienia więcej niż jednego systemu operacyjnego różnych producentów jednocześnie) za pomocą wbudowanego narzędzia * wbudowany system pomocy w języku polskim, * możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).   Klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  W ramach realizacji przedmiotu zamówienia powinna być najnowsza dostępna wersja ww. systemu operacyjnego. |
| **Oprogramowanie biurowe** | Licencja pakietu biurowego zgodnego ze specyfikacją, poz. 9 – Pakiet oprogramowania biurowego.  Oprogramowanie biurowe musi być zainstalowane na każdym z dostarczonych stacjonarnych zestawów komputerowych. |
| **Złącza, porty i wyposażenie** | Wbudowane porty:   * Min. 1 x DP 1.2 * Min. 6 portów USB wyprowadzonych na zewnątrz obudowy komputera, * w tym min. 2 porty USB 3.1; min. 2 porty USB 2.0 usytuowane z tyłu obudowy, * w tym min. 2 porty USB 3.1 usytuowane z boku obudowy;   Wymagana ilość i rozmieszczenie portów USB (na zewnątrz obudowy komputera) nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.  Co najmniej 3 porty USB powinny posiadać opcję szybkiego ładowania urządzeń zewnętrznych.   * Port audio typu combo lub 2 porty audio w kombinacji 1x in i 1x out * Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, z obsługą PXE, WoL, iAMT. * Karta WiFi a/c Wireless 2x2 Dual-Band.   Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w :  min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM 2400MHz,  min. 2 złącza mSATA  min. 1 złącze M.2 PCI-Express x4 dedykowane dla dysku SSD  min. 1 złącze M.2 dedykowane dla karty WiFi   * Klawiatura USB w układzie polski programisty * Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) |
| **Inne wymagania** | Każdy z zestawów komputerowych musi być przygotowany do pracy i zainstalowany na wskazanym przez Zamawiającego stanowisku pracy.  U Zamawiającego pozostaje 1 kompletny karton od zestawów komputerowych. |

|  |  |
| --- | --- |
| 1. **Pakiet oprogramowania biurowego – 33 sztuki** | |
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| **Licencja** | Oprogramowanie winno być dostarczone z bezterminową licencją na użytkowanie |
| **Interfejs użytkownika** | a) pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim;  b) pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim;  c) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;  d) możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0);  e) pakiet aplikacji biurowych powinien prawidłowo współpracować z aplikacjami w modelu chmury obliczeniowej, w szczególności do pracy grupowej i synchronizacji danych |
| **Zawartość pakietu** | Pakiet zintegrowanych aplikacji biurowych musi zawierać:  a) edytor tekstów,  b) arkusz kalkulacyjny,  c) narzędzie do przygotowywania i prowadzenia prezentacji,  d) narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),  e) zainstalowanie na jednym komputerze produktów pochodzących od różnych producentów nie jest uznane za ofertę zintegrowanego pakietu |
| **Edytor tekstów** | Edytor tekstów musi umożliwiać:  a) 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,  b) wstawianie oraz formatowanie tabel,  c) wstawianie oraz formatowanie obiektów graficznych,  d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),  e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,  f) automatyczne tworzenie spisów treści,  g) formatowanie nagłówków i stopek stron,  h) sprawdzanie pisowni w języku polskim,  i) śledzenie zmian wprowadzonych przez użytkowników,  j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,  k) określenie układu strony (pionowa/pozioma),  l) wydruk dokumentów,  m) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego,  n) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,  o) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,  p) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem,  q) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa |
| **Arkusz kalkulacyjny** | Arkusz kalkulacyjny musi umożliwiać:  a) tworzenie raportów tabelarycznych,  b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,  c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,  d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),  e) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,  f) wyszukiwanie i zamianę danych,  g) wykonywanie analiz danych przy użyciu formatowania warunkowego,  h) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,  i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,  j) formatowanie czasu, daty i wartości finansowych z polskim formatem,  k) zapis wielu arkuszy kalkulacyjnych w jednym pliku,  l) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,  m) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji |
| **Narzędzie do przygotowywania i prowadzenia prezentacji** | Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a) przygotowywanie prezentacji multimedialnych, które będą prezentowanie przy użyciu projektora multimedialnego,  b) drukowanie w formacie umożliwiającym robienie notatek,  c) zapisanie jako prezentacja tylko do odczytu,  d) nagrywanie narracji i dołączanie jej do prezentacji,  e) opatrywanie slajdów notatkami dla prezentera,  f) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,  g) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,  h) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,  i) możliwość tworzenia animacji obiektów i całych slajdów,  j) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,  k) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010, |
| **Narzędzie do zarządzania informacją prywatną** | Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,  b) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,  c) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,  d) automatyczne grupowanie poczty o tym samym tytule,  e) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,  f) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia,  g) zarządzanie kalendarzem  h) udostępnianie kalendarza innym użytkownikom,  i) przeglądanie kalendarza innych użytkowników,  j) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,  k) zarządzanie listą zadań,  l) zlecanie zadań innym użytkownikom,  m) zarządzanie listą kontaktów,  n) udostępnianie listy kontaktów innym użytkownikom,  o) przeglądanie listy kontaktów innych użytkowników,  p) możliwość przesyłania kontaktów innym użytkowników, |
| **Inne wymagania** | Pakiet biurowy musi być zainstalowany na wszystkich dostarczonych stacjonarnych zestawach komputerowych. |

|  |  |
| --- | --- |
| 1. **Skaner – 1 sztuka** | |
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| **Typ skanera** | Skaner płaski z automatycznym podajnikiem i funkcją skanowania obydwu stron podczas jednego przebiegu.  Technologia LED zapewniająca szybki czas startu skanowania. |
| **Rozdzielczość optyczna** | Co najmniej 600 dpi x 600 dpi (poziomo x pionowo) |
| **Rozmiar skanowanych dokumentów** | Przy pracy z automatycznego podajnika w zakresie co najmniej:   * od 68 mm x 120 mm (poziomo x pionowo) * do 297 mm x 2.540 mm (poziomo x pionowo)   Gramatura papieru przy pracy z automatycznego podajnika w zakresie co najmniej 40 - 120 g/m².  Akceptowane formaty: B6, B5, B4, A6, A5, A4, A3, Executive, Legal, Letter |
| **Parametry wydajnościowe** | Prędkość skanowania dla dokumentu A4 i rozdzielczości 200 / 300 dpi co najmniej:   * monochromatyczny 70 str./min. i 140 obrazów/min. * kolor 70 str./min. i 140 obrazów/min.   Dzienna wydajność niezawodnej pracy: co najmniej 7500 stron  Pojemność automatycznego podajnika dokumentów: co najmniej 190 stron |
| **Głębia kolorów** | Wejściowa co najmniej:   * tryb monochromatyczny 16 bitów. * tryb kolor 48 bitów.   Wyjściowa co najmniej:   * tryb monochromatyczny 8 bitów. * tryb kolor 24 bity. |
| **Funkcje przetwarzania obrazów** | Co najmniej:   * wykrywanie podwójnego pobrania arkuszy, * pomijanie pustych stron, * rozszerzona edycja obrazu, * wstępnie zdefiniowane ustawienia, * automatyczny podział na obszary, * automatyczna korekta położenia ukośnego, * automatyczne rozpoznawanie dokumentów wielostronicowych, automatyczne wykrywanie trybu czarno-białego i kolorowego, * podwójna edycja obrazu, * automatyczny obrót obrazu, * poprawa tekstu, * wygładzenie krawędzi, * maskowanie nieostrości, * derasteryzacja, * korekcja grzbietu książki, * automatyczne tworzenie folderów, * rozpoznawanie kodu kreskowego, * obsługa strefowego optycznego rozpoznawania znaków OCR A i B, * ręczna i automatyczna separacja zadań. |
| **Pliki wyjściowe** | Formaty pliku wyjściowego co najmniej:   * JPEG, TIFF, * skanowanie do multi-TIFF, PDF, * skanowanie do PDF, * skanowanie do zabezpieczonego PDF, PDF/A.   Funkcje kompresji pliku a co najmniej:   * sprzętowa kompresja JPEG, * kompresja TIFF (JPEG(7), CCITT G4, LZW), * kompresja PDF.   Metody udostępniania pliku wyjściowego:   * skanowanie do e-maila, * skanowanie na FTP, * skanowanie do Microsoft SharePoint®, * skanowanie do drukowania, * skanowanie do katalogu web, * skanowanie do katalogu. |
| **Interfejsy komunikacyjne** | Interfejsy sieciowe:   * Ethernet 10BASE-T/100BASE-TX/1000BASE-T, * WiFi.   Komunikacja z użytkownikiem:   * panel LCD z funkcją skanowanie za pomocą przycisku oraz konfigurowanie funkcji skanowania i udostępniania plików wyjściowych, * praca w sieci, udostępnienie funkcji urządzenia wielu użytkownikom. |
| **Zużycie energii** | Nie więcej niż:   * 85W podczas normalnej pracy, * 20W podczas pracy w trybie ekonomicznym, * 5W w trybie czuwania. |
| **Warunki gwarancji** | Co najmniej 4 lata gwarancji producenta (**nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty**) realizowanej w miejscu instalacji sprzętu, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub system zgłoszeń producenta.  Obsługa gwarancyjna realizowana przez polski oddział serwisu producenta. |
| **Inne wymagania** | Skaner musi być zainstalowany na stanowisku pracy wskazanym przez Zamawiającego i skonfigurowany, gotowy do pracy. |

|  |  |
| --- | --- |
| 1. **Rozbudowa istniejącego UPS o dodatkowe moduły bateryjne – 2 sztuki** | |
| **Nazwa podzespołu** |  |
| **Istniejący UPS** | UPS Eaton PW9130i3000R-XL2U |
| **Dodatkowe zewnętrzne moduły bateryjne rackowe**  **EBM** | Dostawa i instalacja dwóch zewnętrznych modułów bateryjnych instalowanych w racku 19”.  PW9130N3000R-EBM2U 103006460-6591 wymiary: 86,5 x 438 x 600 waga: 41,1 kg |

|  |
| --- |
| 1. **System obejmujący serwer telekomunikacyjny z rejestratorem rozmów – 1 komplet** |

System powinien zawierać wszystkie niezbędne do jego funkcjonowania elementy.

System powinien być w pełni funkcjonalnym i autonomicznym systemem telekomunikacyjnym, niezależnym od infrastruktury operatora telekomunikacyjnego, do której jest podłączony (linii zewnętrznych). Urządzenia i licencje składające się na System będą w stanie realizować wszystkie funkcje łączności wewnętrznej, zarządzania i monitorowania bez potrzeby komunikacji z infrastrukturą operatora lub odwoływania się do jakiegokolwiek urządzenia umieszczonego poza siecią LAN/VPN, a dołączenie do sieci operatora będzie wymagane wyłącznie dla potrzeb realizacji połączeń telefonicznych poza system.

Dostarczony system powinien współpracować prawidłowo z siecią operatora w standardzie: ISDN, POTS oraz obsługiwać współpracę z protokółem SIP, przy założeniu, że operator zapewni interfejsy i protokoły spełniające wymagania zgodne z obowiązującymi w Polsce normami.

Dostarczone rozwiązanie, w celu zapewnienia niezawodności, posiada architekturę, na którą składają się poniższe elementy:

1. Główny serwer – zapewnia zarządzanie całym systemem, obsługę aparatów telefonicznych IP, analogowych, cyfrowych, komunikację z platformą operatora za pomocą linii analogowych, linii cyfrowych ISDN PRA (30B+D), kanałów SIP.
2. Serwer aplikacyjny – 1 szt. (należy dostarczyć, o ile wymagane funkcjonalności nie są realizowane bezpośrednio przez główny serwer telekomunikacyjny lub jest niezbędny do funkcjonowania całego Systemu)
3. Telefon podstawowy – 47 szt.
4. Telefon zaawansowany – 1 szt.

System powinien zapewniać świadczenie dodatkowych usług, np.: zunifikowana komunikacja, poczta głosowa, zapowiedzi IVR, nagrywanie połączeń.

System powinien mieć możliwość rozbudowy o funkcję redundancji, poprzez uruchomienie dodatkowego serwera lub serwerów, umożliwiających przejęcie funkcji zarządzania całym systemem, obsługi aparatów telefonicznych IP, w przypadku wystąpienia awarii Głównego serwera.

System powinien mieć możliwość rozbudowy poprzez dołączenie dodatkowych lokalizacji, wyposażonych w serwery umożliwiające bezpośrednią komunikację i tworzenie jednego logicznego systemu komunikacyjnego, ze wspólną numeracją, wzajemnym przekazywaniem informacji o statusach użytkowników (poprzez prezentowanie tej informacji w aplikacji lub na telefonach użytkowników), tworzeniu rozproszonych grup użytkowników występujących.

Wszystkie elementy systemu powinny posiadać co najmniej 4 lata gwarancji producenta (**nie krócej niż okres gwarancji i wsparcia zadeklarowany w formularzu oferty**).

1. **Główny serwer telekomunikacyjny – 1 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa składnika/parametru technicznego** | | **Minimalne wymagania w zakresie parametrów technicznych** | |
| **Konfiguracja sprzętowa** | | * Konstrukcja nie przekraczająca wysokości 2U umożliwiająca montaż w standardowej szafie rack 19’, * Po obsadzeniu jej odpowiednimi kartami lub modułami, ma możliwość obsługi: * Minimum 1 linia ISDN PRA, * Minimum 2 linie analogowych POTS miejskich * Minimum 2 linie analogowych POTS wewnętrznych * Minimum 100 linii wewnętrznych SIP, z możliwością zwiększenia do min. 2000 bez zakupu dodatkowych modułów lub licencji * Co najmniej dwa porty LAN o przepustowości min. 100 Mbit/s każdy. * Minimum jeden port do zarządzania systemem. Dopuszcza się zarządzanie w paśmie poprzez porty LAN. * Posiada na froncie urządzenia wyświetlacz lub wskaźniki LED sygnalizujące stan pracy systemu. * Posiada budowę modularną umożliwiającą zainstalowanie modułów lub podłączenie bramek zewnętrznych do obsługi dodatkowych portów analogowych, cyfrowych, telefonii IP. | |
| **Wymagania funkcjonalne** | | * Budowa hybrydowa umożliwiająca realizowanie połączeń telekomunikacyjnych zarówno w zakresie tradycyjnej telefonii TDM jak i telefonii IP, * Budowa modułowa lub możliwość podłączenia bramek zewnętrznych umożliwiających dostosowywanie systemu do zmieniających się wymagań a w szczególności zwiększenia lub zmiany liczby portów oraz łączy komunikacyjnych. * Możliwość wyboru komunikacji z siecią publiczną za pomocą linii analogowych, ISDN 30B+D, SIP. * Obsługa telefonów cyfrowych, IP, SIP, DECT, IP DECT oraz aplikacji typu softphone przeznaczonych na komputery stacjonarne oraz smartfony. * Funkcjonalność automatycznej dystrybucji aktualizacji oprogramowania telefonów IP. * Możliwość uruchomienia szyfrowania komunikacji (zarówno sygnalizacji – TLS jak i pakietów głosowych SRTP) z aparatami telefonicznymi IP (SIP) wspierającymi tę funkcjonalność. * Możliwość rozbudowy systemu do co najmniej 300 abonentów dowolnego typu telefonów (analogowe, cyfrowe, IP) oraz 1000 użytkowników w przypadku kilku serwerów pracujących w sieci w skali całego systemu i wszystkich lokalizacji łącznie. * Możliwość obsługi łączy SIP do operatora telekomunikacyjnego o pojemności minimum 100 jednoczesnych rozmów. * Wsparcie i pełną obsługę dla kodeków: G722, G711, G729 oraz protokołu T.38. * Wyposażony w mechanizm automatycznego kierowania połączeniami, pozwalający na kierowania rozmów na podstawie czasu i numerów. * Możliwość zdefiniowania numerów alarmowych, które będą osiągalne niezależnie od blokad ustanowionych dla telefonu. * Posiada funkcjonalność centralnej książki telefonicznej o pojemności co najmniej 2000 wpisów. * Posiada funkcjonalność list ostatnio zrealizowanych połączeń. * Pozwala na dowolne definiowanie mechanizmu kierowania połączeń przychodzących, według numeru dzwoniącego, numeru wybranego, linii, daty, godziny. * Posiada możliwość zdefiniowania co najmniej 300 grup dzwoniących. * Posiada możliwość kolejkowania połączeń przychodzących do grupy, z opcjonalnymi komunikatami głosowymi dla oczekujących. * Posiada możliwość realizacji połączeń konferencyjnych (min. 16 abonentów w ramach jednej telekonferencji), inicjowanych z poziomu aparatu abonenta lub wdzwaniania się do systemu (minimalna ilość kanałów konferencyjnych – 64) * Posiada funkcję przejęcia połączeń sygnalizowanych u innego abonenta. * Posiada funkcje przekierowania połączeń: bezwarunkowych, w przypadku nieodebrania, w przypadku zajętości, z możliwością uruchomienia funkcji z poziomu telefonu abonenta. * Posiada możliwość definiowania profili czasowych, dla potrzeb kierowania rozmowami oraz określania blokad połączeń. | |
| **Zarządzanie i diagnostyka** | | System umożliwia centralne zarządzanie, diagnostykę oraz monitoring za pomocą aplikacji instalowanych na stacji roboczej z systemem Windows – bez ograniczeń licencyjnych co do liczby zainstalowanych stanowisk. Oprogramowanie posiada następujące funkcjonalności:   * Centralne zarządzanie wszystkimi elementami. * Zarządzanie parametrami aparatów IP / aparatów systemowych w zakresie uruchamiania / wyłączania funkcji oraz programowania przycisków funkcyjnych bez konieczności logowania się do konkretnego aparatu IP. * Zarządzanie abonentami, grupami, aparatami telefonicznymi * Zarządzanie książką telefoniczną * Zarządzanie ustawieniami bezpieczeństwa * Monitoring i diagnostyka w czasie rzeczywistym poszczególnych elementów Systemu telekomunikacyjnego. * Możliwość zdalnego restartu lub zamknięcia wybranych elementów Systemu * Możliwość wykonywania kopii zapasowych konfiguracji. | |

1. **Serwer aplikacyjny – 1 szt. (należy dostarczyć w przypadku, o ile wymagane funkcjonalności nie są realizowane bezpośrednio przez główny serwer telekomunikacyjny lub jest niezbędny do funkcjonowania całego Systemu)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa składnika/parametru technicznego** | | **Minimalne wymagania w zakresie parametrów technicznych** | |
| **Wymagania sprzętowe** | | * Serwer aplikacyjny powinien zostać zainstalowany na maszynie fizycznej lub wirtualnej, którą należy przewidzieć jako element całego rozwiązania. * Powinien pozwalać na nagrywanie rozmów w okresie 30 dni. * Wszystkie funkcje (poniżej opis) powinny działać wydajnie z max. opóźnieniem 1 s, bez odczuwalnych dla użytkownika opóźnień. | |
| **Wymagania funkcjonalne** | | * Funkcja centralnego (dostępnego dla wszystkich elementów systemu) systemu zapowiedzi głosowych. * Poczta głosowa dla każdego użytkownika.   Funkcjonalność systemu nagrywania rozmów, obejmuje:   * Zdolność do nagrywania rozmów wewnętrznych i zewnętrznych, wraz ze szczegółową informacją o stronach połączenia, dacie, godzinie, czasie trwania rozmowy. * Dostęp do odsłuchu nagrań za pomocą interfejsu Web lub dedykowanej aplikacji na komputery z systemem Microsoft Windows, z możliwością utworzenia wielu kont dostępowych dla użytkowników z różnym poziomem uprawnień. * Możliwość eksportu nagrań do plików WAV. * Możliwość rozbudowy liczby kanałów (liczby jednocześnie rejestrowanych rozmów) do minimum 40.   Poprzez wykupienie dodatkowych licencji dla użytkowników system powinien posiadać następujące możliwości:   * Możliwość definiowania min. 8 osobistych pokoi konferencyjnych dla abonentów przez administratora serwera lub użytkownika z specjalnymi uprawnieniami. * Aplikacja dla urządzeń mobilnych działających, umożliwiającą: realizację połączeń i transmisję głosu z użyciem danych pakietowych, dostęp do książki telefonicznej, zarządzania pocztą głosową i konferencją. | |

1. **Telefon podstawowy – 47 sztuk**

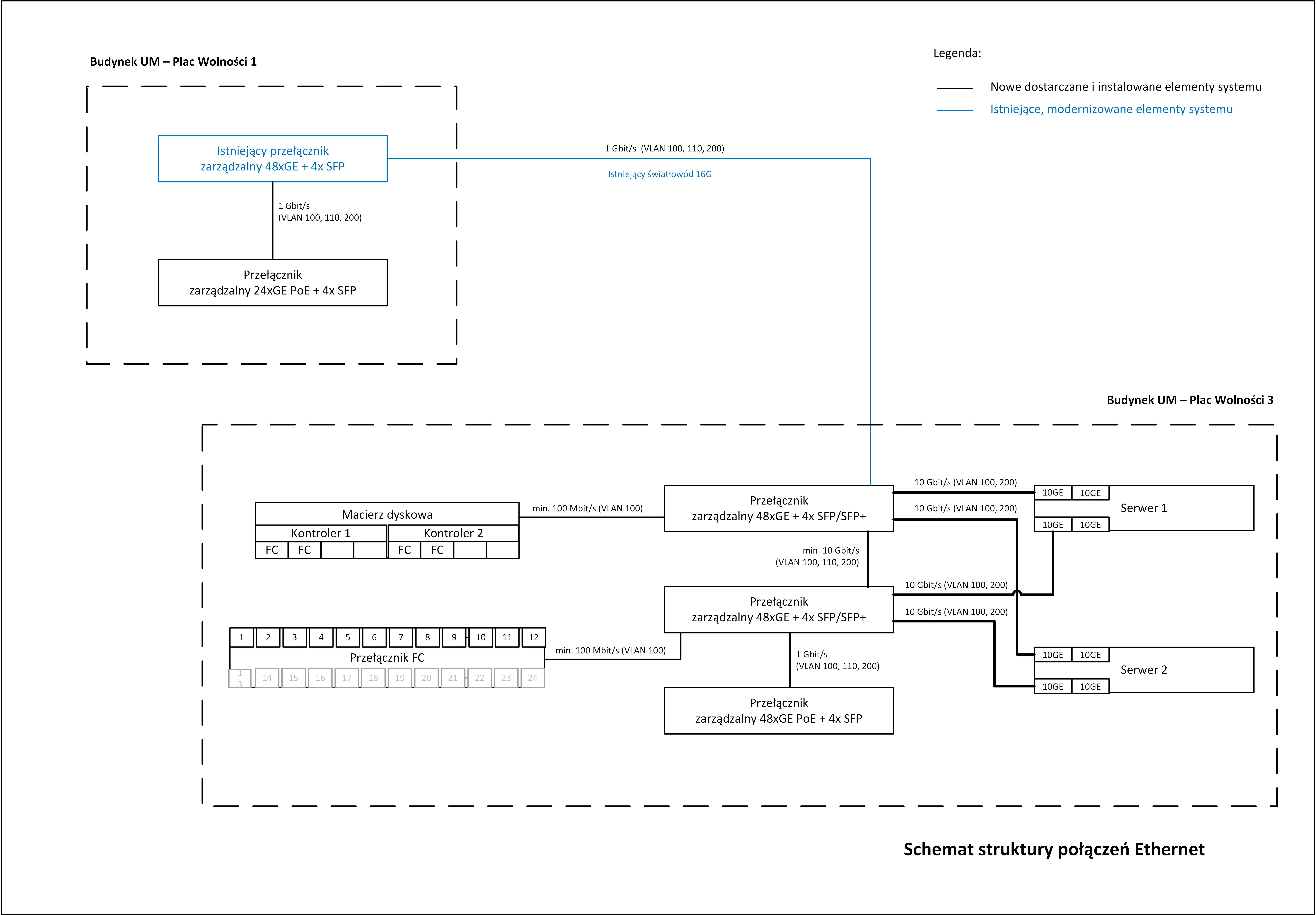
|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa składnika/parametru technicznego** | | **Minimalne wymagania w zakresie parametrów technicznych** | |
| **Cechy i funkcje** | | * Wyświetlacz z możliwością wyświetlenia co najmniej 3 linii znaków, podświetlany * Przycisk nawigacyjny 4-kierunkowy + przycisk potwierdzenia do obsługi funkcji aparatu telefonicznego. * Menu aparatu dostępne w wielu językach, w tym w języku polskim. * 8 konfigurowalnych przycisków szybkiego wyboru z diodą LED sygnalizującą zajętość numeru lub włączenie funkcji przypisanej do przycisku * Na stałe skonfigurowane są przyciski funkcji: * Włączenie systemu głośnomówiącego * Mute – wyłączenie mikrofonu * Książka telefoniczna * Przycisk lub dynamicznie programowalny przycisk dostępu do list połączeń (w tym listy nieodebranych połączeń) * Przycisk lub dynamicznie programowalny przycisk wyjścia / przejścia do głównego ekranu telefonu. * Funkcje związane z obsługą połączenia, dostępne w formie stałych przycisków lub dynamicznych przycisków programowych (tzw. Soft-key):  1. Hold – zawieszenie aktualnie trwającego połączenia. 2. Konsultacja – zawieszenie istniejącego połączenia w celu wykonania drugiego 3. Transfer – przekazanie rozmowy do innego abonenta 4. Konferencja  * Dioda LED sygnalizująca pozostawioną wiadomość w poczcie głosowej oraz nadejście połączenia przychodzącego. * Wbudowany mikrofon i głośnik umożliwiający rozmowę bez podniesionej słuchawki, * Przycisk lub elektroniczny potencjometr do regulacji głośności: słuchawki, głośnika, zestawu nagłownego oraz głośności wywołania. * Port Ethernet o przepustowości min. 10/100 Mbps do komunikacji z przełącznikiem sieciowym oraz zasilania * Dodatkowy port Ethernet o przepustowości min. 10/100 Mbps np. do podłączenia komputera PC. * Dedykowany (dodatkowy) port do podłączenia zestawu nagłownego * Wsparcie dla kodeków: G.711, G.729. * Wsparcie dla Quality of Service (QoS) z wykorzystaniem 802.1p i/lub DiffServ, * Wsparcie dla VLAN * Obsługa LLDP, LLDP-MED w celu zautomatyzowanej konfiguracji parametrów wstępnych aparatu, takich jak VLAN, czy polityki QoS. * Zasilanie z użyciem PoE 802.3af | |
| **Współpraca z systemem** | | * Obsługa wielu linii i jednoczesnych połączeń, wraz z prezentacją statusu połączenia na wyświetlaczu telefonu. * Możliwość zestawienia połączenia konferencyjnego * Możliwość konfigurowania przycisków aparatu oraz funkcji takich jak: nie przeszkadzać, przekierowania połączeń z poziomu aparatu, wraz z powiadomieniem o włączonej funkcji (np. „Nie przeszkadzać”, to na aparacie zostanie wyświetlona stosowna informacja). * Przechowywanie ustawień aparatu telefonicznego (ustawień funkcji połączeń, przycisków funkcyjnych) – po zmianie aparatu na inny egzemplarz i wprowadzeniu poświadczeń, w/w ustawienia powinny zostać skopiowane. | |

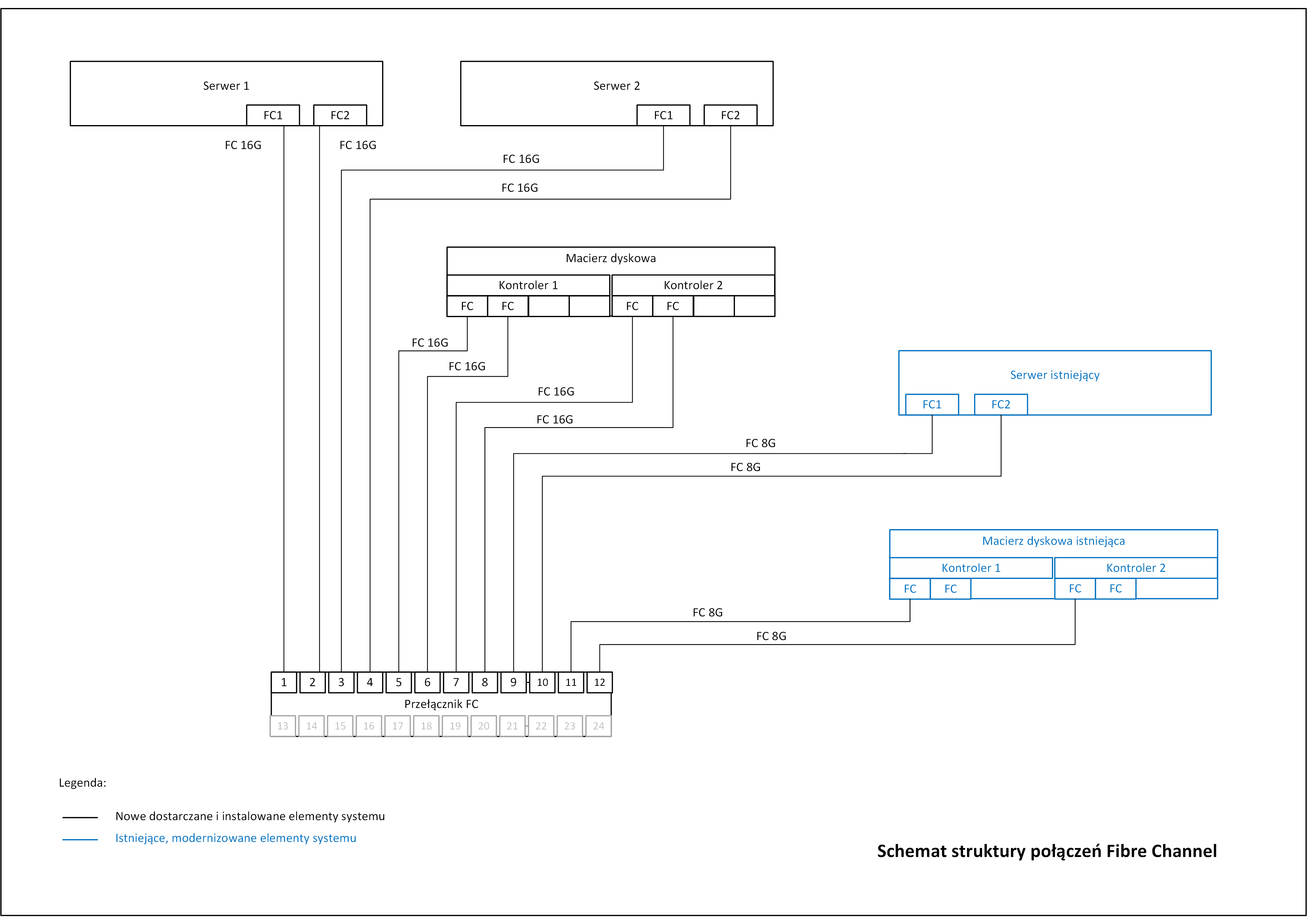
1. **Telefon zaawansowany – 1 sztuka**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa składnika/parametru technicznego** | | **Minimalne wymagania w zakresie parametrów technicznych** | |
| **Cechy i funkcje** | | * Wyświetlacz graficzny, podświetlany, o przekątnej przynajmniej 3 cale. * Przycisk nawigacyjny 4-kierunkowy + przycisk potwierdzenia do obsługi funkcji aparatu telefonicznego. * Menu aparatu dostępne w wielu językach, w tym w języku polskim. * Obsługa min. 40 linii wewnętrznych za pomocą konfigurowalnych przycisków (dostępnych bezpośrednio w aparacie lub za pośrednictwem dostarczonej razem z telefonem przystawki rozszerzającej) szybkiego wyboru z dwukolorowymi diodami LED sygnalizującymi zajętość numeru lub włączenie funkcji przypisanej do przycisku (Busy Lamp Field (BLF), Call Park, Conference, Intercom, Monitor Call park, Transfer, Speed Dial, Redial, Presence, itp. – możliwe do przypisania do dowolnego z przycisków) oraz wyświetlaczem LCD o rozdzielczości min. 100 x 350 pikseli wyświetlającym nazwę przypisanego abonenta lub funkcję. * Na stałe skonfigurowane musza być przyciski funkcji:   + Włączenie systemu głośnomówiącego   + Mute – wyłączenie mikrofonu   + Książka telefoniczna   + Przycisk lub dynamicznie programowalny przycisk dostępu do list połączeń (w tym listy nieodebranych połączeń)   + Przycisk lub dynamicznie programowalny przycisk wyjścia / przejścia do głównego ekranu telefonu. * Funkcje związane z obsługą połączenia, dostępne w formie stałych przycisków lub dynamicznych przycisków programowych (tzw. Soft-key):  1. Hold – zawieszenie aktualnie trwającego połączenia. 2. Konsultacja – zawieszenie istniejącego połączenia w celu wykonania drugiego 3. Transfer – przekazanie rozmowy do innego abonenta 4. Konferencja  * Dioda LED sygnalizująca pozostawioną wiadomość w poczcie głosowej oraz nadejście połączenia przychodzącego. * Wbudowany mikrofon i głośnik umożliwiający rozmowę bez podniesionej słuchawki, * Przycisk lub elektroniczny potencjometr do regulacji głośności: słuchawki, głośnika, zestawu nagłownego oraz głośności wywołania. * Port Ethernet o przepustowości 10/100/1000 Mbit/s do komunikacji z przełącznikiem sieciowym oraz zasilania * Dodatkowy port Ethernet o przepustowości 10/100/1000 Mbps np. do podłączenia komputera PC. * Dedykowany (dodatkowy) port do podłączenia zestawu nagłownego * Wsparcie dla kodeków: G.711, G.729, * Możliwość podłączenia min. czterech przystawek rozszerzających wyboru bezpośredniego z dodatkowymi przyciskami z dwukolorowymi diodami LED oraz wyświetlaczem LCD o rozdzielczości min. 100 x 350 pikseli, umożliwiające wybór bezpośredni min. 150 abonentów i/lub funkcji * Wsparcie dla Quality of Service (QoS) z wykorzystaniem 802.1p i/lub DiffServ, * Wsparcie dla VLAN * Obsługa LLDP, LLDP-MED w celu zautomatyzowanej konfiguracji parametrów wstępnych aparatu, takich jak VLAN, czy polityki QoS. * Zasilanie z użyciem PoE 802.3af | |
| **Współpraca z systemem** | | * Obsługa wielu linii i jednoczesnych połączeń, wraz z prezentacją statusu połączenia na wyświetlaczu telefonu. * Możliwość zestawienia połączenia konferencyjnego * Możliwość konfigurowania przycisków aparatu oraz funkcji takich jak: nie przeszkadzać, przekierowania połączeń z poziomu aparatu, wraz z powiadomieniem o włączonej funkcji (np. „Nie przeszkadzać”, to na aparacie zostanie wyświetlona stosowna informacja). * Przechowywanie ustawień aparatu telefonicznego (ustawień funkcji połączeń, przycisków funkcyjnych) – po zmianie aparatu na inny egzemplarz i wprowadzeniu poświadczeń, w/w ustawienia powinny zostać skopiowane. | |

|  |
| --- |
| 1. **Wymagany schemat połączeń wyposażenia serwerowni** |

Dostarczone elementy wyposażenia serwerowni powinny zostać połączone zgodnie z poniższymi schematami.





Wykonawca dostarczy wszelkie niezbędne elementy połączeniowe pomiędzy urządzeniami, tj. moduły transmisyjne, patchcordy, itp. zapewniające zestawienie połączeń pomiędzy urządzeniami o wymaganych przepływnościach.

|  |
| --- |
| 1. **Wymagania w zakresie szkolenia administratorów** |

W ramach realizacji przedmiotu zamówienia Wykonawca przeszkoli 2 administratorów w zakresie:

* administrowania systemami serwerowymi i bazodanowymi,
* zarządzania dostarczonymi urządzeniami,
* kompleksowego system bezpieczeństwa i zarządzania infrastrukturą

**16. Lista lokalizacji instalacji 33 zestawów komputerowych**

|  |  |  |
| --- | --- | --- |
| **l.p.** | **Lokalizacja** | **Ilość zestawów komputerowych** |
| 1 | Plac Wolności 3, Urząd Miejski w Olecku | 15 |
| 2 | Plac Wolności 1, Urząd Miejski w Olecku | 5 |
| 3 | Szkoła Podstawowa w Judzikach, Judziki 5, 19-400 Olecko | 1 |
| 4 | Szkoła Podstawowa w Babkach Oleckich, Babki Oleckie 12, 19-400 Olecko | 1 |
| 5 | Szkoła Podstawowa w Kijewie, Kijewo 29, 19-404 Wieliczki | 1 |
| 6 | Miejski Ośrodek Sporu i Rekreacji, ul. Park 1, 19-400 Olecko | 1 |
| 7 | Szkoła Podstawowa Nr 2, ul. Słowiańska 1, 19-400 Olecko | 1 |
| 8 | Warsztat Terapii Zajęciowej w Olecku, ul. Kopernika 6, 19-400 Olecko | 1 |
| 9 | Regionalny Ośrodek Kultury w Olecku "Mazury Garbate", Plac Wolności 22, 19-400 Olecko | 1 |
| 10 | Szkoła Podstawowa w Gąskach, Gąski 14, 19-400 Olecko | 1 |
| 11 | Przedszkole z Oddziałami Integracyjnymi KRASNAL w Olecku, ul. Zielona 1, 19-400 Olecko | 1 |
| 12 | Szkoła Podstawowa nr 3 w Olecku, ul. Kolejowa 33, 19-400 Olecko | 1 |
| 13 | Miejski Ośrodek Pomocy Społecznej, ul. Kolejowa 31, 19-40 0 Olecko | 1 |
| 14 | Szkoła Podstawowa nr 1 w Olecku, ul. Kościuszki 20, 19-400 Olecko | 1 |
| 15 | Szkoła Podstawowa Nr 4 w Olecku, Osiedle Siejnik I 14, 19-400 Olecko | 1 |