**Specyfikacja**

**na dostawę i instalację infrastruktury teleinformatycznej i architektury technicznej**

**Specyfikacja przedmiotu zamówienia w obszarze infrastruktury teleinformatycznej.**

**dla Instytutu Gruźlicy i Chorób Płuc Oddział Terenowy w Rabce-Zdrój**

# Specyfikacja dostarczanej infrastruktury informatycznej i architektury technicznej.

W poniższej tabeli przedstawiono typy oraz liczbę zamawianej infrastruktury teleinformatycznej.

Tabela 1. Typy oraz liczba zamawianej infrastruktury teleinformatycznej.

| **Typ** | **Liczba zamawianego sprzętu (sztuk)** |
| --- | --- |
| Baza danych | 1 |
| Serwer backupowy | 1 |
| Przełącznik dystrybucyjny | 9 |
| Moduły SFP+ do przełączników dystrybucyjnych | 14 |
| Moduły SFP+ do przełączników dystrybucyjnych | 4 |
| Napęd taśmowy z taśmą | 1 |
| Tablety medyczne – typ 1 | 6 |
| Tablety medyczne – typ 2 | 6 |
| Laptop | 3 |
| Punkt dostępowy Wifi | 15 |
| Terminal komputerowy | 30 |
| Komputer stacjonarny z monitorem i oprogramowaniem | 30 |
| Duplikator DVD | 1 |
| Czytnik kodów kreskowych | 9 |
| Drukarka kodów kreskowych | 4 |
| Urządzenie wielofunkcyjne  – typ 1 | 2 |
| Urządzenie wielofunkcyjne  – typ 2 | 10 |
| UTM | 2 |
| Szafa serwerowa | 1 |
| Licencja dostępowa | 30 |
| Oprogramowanie backupowe | 2 |
| System typu NAC (Network Access Control) | 1 |

W poniższej tabeli przedstawiono szczegóły dotyczące planowanej do zamówienia infrastruktury teleinformatycznej.

Tabela 2. Szczegóły zamawianej infrastruktury teleinformatycznej w podziale na komponenty.

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Baza danych** | | |
| 1. | Licencje bazy danych | 1. Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX dla procesorów POWER, Intel/AMD Linux, MS Windows). Identyczna funkcjonalność serwera bazy danych na ww. platformach 2. Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, etc. Licencje nie mogą być ograniczone czasowo. 3. Proponowany zestaw licencji powinien być jednorodny. Wymagana jest dostawa oprogramowania certyfikowanego pod względem zgodności ze sobą. Wymaganie obejmuje: 4. Oprogramowanie bazy danych ze względu na zgodność z systemem operacyjnym oraz platformą sprzętową, 5. Systemy operacyjne używane do uruchamiania serwerów bazy danych ze względu na zgodność z platformą sprzętową. 6. Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu), wymaganie nie musi zostać spełnione w przypadku dostarczenia oprogramowania działającego w oparciu o jedną bazę danych. 7. Oprogramowanie klienckie, za pomocą, którego można łączyć się do bazy danych musi być dostępne na wielu platformach systemowo-sprzętowych (minimalny zakres platform taki jak dla oprogramowania serwera bazy danych) 8. Wsparcie protokołu XA. 9. Wsparcie standardu JDBC 3.0. 10. Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. 11. Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. 12. RDBMS musi zapewniać niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych. 13. RDBMS musi zapewniać przetwarzanie transakcyjne wg reguł ACID z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji musi pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, spójny odczyt nie może blokować możliwości wykonywania zmian. 14. RDBMS musi posiadać możliwość zagnieżdżania transakcji – Możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. 15. Dostępność poziomu serializowanego poziomu izolowania transakcji (Serializable). 16. Możliwość zmiany domyślnego trybu izolowania transakcji (Read Commited) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych. 17. Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode) zarówno po stronie serwera bazy danych jak i oprogramowania klienckiego. Wsparcie dla polskich stron kodowych – ISO-8859-2, MS Windows Code Page 1250 oraz PC 852. Automatyczna konwersja znaków pomiędzy różnymi ustawieniami stron kodowych po stronie klienta i serwera bazy danych. 18. Możliwość migracji bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode. 19. Możliwość definiowania w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku. 20. Możliwość bez dodatkowych ograniczeń przechowywania wierszy, których rozmiar przekracza rozmiar bloku bazy danych. 21. Możliwość budowania indeksów o strukturze B-drzewa. Baza danych powinna umożliwiać założenie indeksu jednej lub większej liczbie kolumn tabeli, przy czym ograniczenie liczby kolumn, na których założony jest 1 indeks nie powinno być mniejsze niż 16. 22. Możliwość budowania widoków zmaterializowanych odzwierciedlających stan danych zdefiniowanych przez zapytanie SQL. Widok zmaterializowany przechowuje rezultat zapytania, którego aktualizacja odbywa się w jednej z dostępnych strategii – na żądanie, okresowo bądź po każdym zatwierdzeniu transakcji modyfikującej tabele, na której oparty jest widok zmaterializowany. 23. Możliwość szybkiego odświeżania danych w widoku zmaterializowanym na podstawie mechanizmu identyfikacji zmian w danych źródłowych. 24. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). 25. Kosztowy model optymalizacji instrukcji SQL. 26. Model statystyk optymalizatora kosztowego musi pozwalać na odwzorowanie nierównomierności rozkładu danych (składowanie informacji o rozkładzie wartości występujących w kolumnach za pomocą histogramu bądź porównywalnego funkcjonalnie modelu odwzorowania). 27. Możliwość uwzględnienia korelacji wartości występujących w niezależnych kolumnach tabeli w modelu statystyk optymalizatora kosztowego. 28. RDBMS powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć Możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL. 29. Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. 30. Procedury i funkcje składowane powinny mieć Możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć Możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury). 31. Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej). 32. W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji, w której wystąpił ww. błąd lub wyjątek. 33. Możliwość wykonania równoczesnych operacji DML (Insert/Update/Delete) na tej samej tabeli. 34. Powinna istnieć Możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu zewnętrznego w stosunku do bazy danych. 35. Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. 36. Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, itp.). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online(hot backup). 37. Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. 38. Możliwość uruchomienia bazy danych w środowisku klastra wielu aktywnych serwerów bazy danych. 39. Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej bazy danych (struktura plików danych). 40. Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji logicznej struktury baz danych (tabel / indeksów). 41. Unieruchomienie jednego z serwerów klastra bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów. 42. Możliwość kontynuacji pracy użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Wymagana jest Możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia. 43. Każdy z serwerów klastra musi mieć Możliwość uspójnienia lub odtworzenia całej bazy danych w sytuacji awarii nośników lub nagłego zatrzymania innego serwera, który utrzymywał w buforze bazy danych zmodyfikowane, ale niezapisane bloki danych. 44. Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera, do którego zostało nawiązane połączenie. 45. Część funkcjonalna lub rozszerzenie serwera bazy danych, musi działać na platformach sprzętowych i systemowych wspieranych przez bazę danych; pozwalająca na uruchomienie bazy w środowisku klastra wielu aktywnych serwerów bazy danych. 46. Dopuszcza się istnienie dodatkowej przestrzeni tabel w ramach instalacji, w której użytkownik będzie mógł przechowywać dane zapytań, własne procedury, funkcje, tabele itp. Dopuszczalne będzie odpytywanie wykorzystywanej bazy danych. 47. Licencja bazy danych jest bezterminowa. Prawa do aktualizacji wygasają po upływie 5 lat od daty zakupu. Możliwość przedłużenia gwarancji. |
| **Serwer backupowy** | | |
|  | Obudowa | Jednostka główna maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)  Serwer z dostępnym, jako opcja (możliwość instalacji), zdejmowanym panelem przedni wyposażonym w zamek i chroniącym przed nieuprawionym dostępem do dysków oraz czujnik otwarcia obudowy współpracującego z BIOS/UEFI. |
|  | Procesor | Procesor szesnastordzeniowy, x86 - 64 bity, Intel Xeon 6242 lub równoważne procesory szesnastordzeniowe pracujące z częstotliwością bazową min.2.8GHz i osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 216 punktów, dla testu oferowanego modelu serwera  z 2 procesorami.  W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.spec.org  Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz. |
|  | Liczba procesorów | 1 procesor, możliwość rozbudowy o dodatkowy procesor |
|  | Pamięć operacyjna i płyta główna | Min. 256 GB RDIMM/LRDIMM DDR4 2933 MT/s w modułach pamięci o pojemności min. 64GB każdy  Płyta główna z minimum 24 slotami na pamięć, umożliwiająca instalację minimum 3TB (przy zastosowaniu odpowiednich procesorów).  Obsługa zabezpieczeń: Advanced ECC i Online Spare. |
|  | Sloty rozszerzeń | Min. 3 aktywne gniazda PCI-Express generacji 3 pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width). Wszystkie sloty umożliwiające instalacje kart pełnej wysokości.   * Możliwość rozbudowy do min. 6 slotów PCI-Express generacji 3 pełnej wysokości (full height) do obsadzenia kartami z portami zewnętrznymi. Rozbudowa przy pełnej obsadzie procesorów. * Możliwość rozbudowy/rekonfiguracji serwera do min. 5 slotów PCI-Express x 16 (przepustowość gniazda x16) generacji 3 pełnej wysokości i długości (full height, full length). Rozbudowa/rekonfiguracja przy pełnej obsadzie procesorów. |
|  | Zasoby dyskowe | Zatoki dyskowe z przodu serwera, gotowe do zainstalowania min. 12 dysków typu Hot Swap, SAS/SATA/SSD 3,5”.  Min. 2 zatoki dyskowe z przodu lub z tyłu serwera, gotowe do zainstalowania dysków typu Hot Swap SAS/SATA/SSD 2,5”.  Zainstalowane:   * min. 12 x 4TB SAS 7.2k 3.5” typu Hot Swap, * min. 2 x 480 GB SSD SATA MU (Mixed Use) typu Hot Swap. |
|  | Kontroler | Serwer wyposażony w:   * Kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min.16 portowy (16 dedykowanych linii SAS do podłączenia dysków SAS), obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler dedykowany do obsługi dysków zainstalowanych w serwerze. * Kontrolery umożliwiające pracę z dyskami w trybach RAID i JBOD jednocześnie. * Kontrolery z możliwością rozbudowy o funkcjonalność szyfrowania wolumenów logicznych stworzonych na podłączonych dyskach (szyfrowanie realizowane przez kontroler RAID, a nie przez oprogramowanie zainstalowane na systemie operacyjnym) lub kontrolery z funkcją współpracy z dyskami samoszyfrującymi SED. W przypadku zastosowania kontrolera RAID z funkcją współpracy z dyskami samoszyfrującymi SED wszystkie zastosowane/dostarczone dyski muszą być dyskami SED. * Dodatkowy kontroler SAS umożliwiający podłączenie i poprawne działanie oferowanej biblioteki wraz z odpowiednim kablem SAS min. 2m. |
|  | Interfejsy sieciowe | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. |
|  | Dodatkowy interfejs sieciowy | Konwergentna karta 4 portowa 10Gb Eth Base-T niezajmująca slotów PCI-E opisanych w punkcie sloty roszerzeń. |
|  | Karta graficzna | Zintegrowana karta graficzna |
|  | Porty | 4 x USB 3.0 (w tym 2 porty wewnętrzne)  1x VGA  Wewnętrzny slot na kartę micro SD.  Możliwość rozbudowy/rekonfiguracji o:  Port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express. |
|  | Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800 W. |
|  | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
|  | Karta/moduł zarządzający | Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:   * monitorowanie podzespołów serwera: wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), * wsparcie pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP * dostęp do karty zarządzającej poprzez   + dedykowany port RJ45 z tyłu serwera lub   + przez współdzielony port zintegrowanej karty sieciowej serwera   dostęp do karty możliwy:   * + z poziomu przeglądarki webowej (GUI)   + z poziomu linii komend   + poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)   + obsługa HTML 5 * wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * zdalna aktualizacja oprogramowania (firmware) * wsparcie dla Microsoft Active Directory * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API * możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) * monitorowanie podzespołów serwera: temperatura, zasilacze, * możliwość zablokowania dokonania obniżenia wersji oprogramowania układowego (firmware) serwera * możliwość równoczesnej obsługi przez min.2 administratorów * obsługa TLS i SSH * zarządzanie grupami serwerów, w tym:   + tworzenie i konfiguracja grup serwerów   + sterowanie zasilaniem (wł/wył)   + ograniczenie poboru mocy dla grupy (power caping)   + aktualizacja oprogramowania (firmware)   + wspólne wirtualne media dla grupy |
|  | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2016 i nowsze  Red Hat Enterprise Linux (RHEL) 7.X lub nowszy  SUSE Linux Enterprise Server (SLES) 12 lub nowszy  VMware ESXi 6.5 lub nowsze |
|  | Karta SAS | Karta rozszerzeń SAS 12Gb z możliwością podłączenia zewnętrznej biblioteki taśmowej ( interfejsie SAS) . |
|  | System operacyjny | System operacyjny Windows Server 2019 Standard lub równoważny, Licencje na wymaganą liczbę rdzeni procesorowych. Licencja z prawem do aktualizacji do następnej wersji systemu operacyjnego. |
|  | Wsparcie techniczne | 3-letnia gwarancja producenta w miejscu instalacji. Zgłoszenia przyjmowane w trybie 9x5 (od poniedziałku do piątku w godzinach 8-17), czas reakcji w następnym dniu roboczym od zgłoszenia. Uszkodzone dyski zostają u Zamawiającego.  Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. |
|  | Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normamą ISO 9001 lub równoważną.  Deklaracja zgodności CE. |
| **Przełącznik dystrybucyjny** | | |
|  | Obudowa | Przełącznik musi posiadać obudowę wolnostojącą, umożliwiająca montaż w 19-calowym stelażu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie) |
|  | Ilość portów | Min 48 portów RJ-45 auto-negotiating 10/100/1000 PoE+ (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3af PoE, IEEE 802.3at)  Min 2 stałe porty SFP+ 1000/10000 SFP+  Min 2 porty RJ-45 1/10GBASE-T |
|  | Dodatkowe porty | Min 1 port RJ45 do zarządzania poprzez konsolę |
|  | Zarządzanie | Musi priorytetyzować pakiety na podstawie DSCP lub IEEE 802.1p (np. Dla VoIP i VIDEO)  Musi zarządzać przepustowością danej transmisji  Musi obsługiwać Class of Service (CoS) |
|  | Zarządzanie jakością (QoS) | Musi priorytetyzować pakiety na podstawie DSCP lub IEEE 802.1p (np. Dla VoIP i VIDEO)  Musi zarządzać przepustowością danej transmisji  Musi obsługiwać Class of Service (CoS) |
|  | Warstwa przełączania | Przepustowość Min. 130,9 Mpps dla 48 portowych  Prędkość przełączenia Min. 176Gbps dla 48 portowych  Opóźnienia: Dla 100Mbps nie więcej niż 5 µs;  Dla 1000Mbps nie więcej niż 5 µs;  Wielkość tablicy MAC:  Min. 16t384  Obsługa ramek Jumbo: Min 10k bajtów  Ilość obsługiwanych Vlanów: min. 4094  Auto MDIX/ Musi obsługiwać automatyczne dostosowanie prędkości i typu połączenia na portach 10/100/1000  Agregacja portów: zgodna z 802.3ad LACP |
|  | Pamięć | Co najmniej 1GB SDRAM, min. 128MB flash; |
|  | Funkcje wysokiej dostępności | Musi obsługiwać następujące protokoły:  - Spanning Tree (802.1d),  - Rapid Convergence Spanning Tree (802.1w),  - Muliple Spanning Trees (802.1s) |
|  | Bezpieczeństwo | W ramach bezpieczeństwa musi obsługiwać:  - SSL,  - https,  - ACL  - STP BPDU port protection  - STP root guard  - logowanie po IEEE 802.1X i RADIUS  - DoS (Automatic)  - Management password  - Automatic VLAN Assignment |
|  | Monitorowanie | Musi obsługiwać:  - denial-of-service protection  - Port mirroring  - RMON |
|  | Pozostałe funkcje | Przełącznik musi dodatkowo obsługiwać:  - funkcję Dual Flash Images – pierwotne i wtórne pliki systemu operacyjnego do tworzenia kopii zapasowych podczas aktualizacji;  - Network Time Protocol (NTP)  - Energy Efficient Ethernet  - Management password  - LLDP-MED  - LLDP  - IGMP/MLD snooping  - DHCP relay  - Auto Voice VLAN  - wsparcie dla FTP,  - możliwość stackowania do 4 urządzeń w stosie  - Packet storm protection |
|  | Oprogramowanie | Urządzenie musi mieć zapewnione bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta |
|  | Informacje dodatkowe | - Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji producenta.  - Wszystkie przełączniki i akcesoria (np. moduły SFP) muszą pochodzić od jednego producenta  - Wszystkie przełączniki muszą być fabrycznie nowe |
|  | Gwarancja | 3 letnia gwarancja producenta zapewniająca dostarczenie sprawnego sprzętu na „podmianę” uszkodzonego, na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia.. |
| **Moduły SFP+ dla przełączników dystrybucyjnych** | | |
|  | Typ interfejsu | SFP+ |
|  | Maksymalna szybkość przesyłania danych | 10000 Mbit/s |
|  | Złącze światłowodowe | LC |
|  | Maksymalny dystans transferu | 300 m |
|  | Typ transceivera SFP | Fiber optic |
|  | Inne | W pełni kompatybilne z zakupywanymi przełącznikami dystrybucyjnymi. |
| **Moduły SFP+ dla przełączników dystrybucyjnych** | | |
|  | Typ interfejsu | SFP+ |
|  | Maksymalna szybkość przesyłania danych | 10000 Mbit/s |
|  | Złącze światłowodowe | LC |
|  | Maksymalny dystans transferu | 2000 m |
|  | Typ transceivera SFP | Fiber optic |
|  | Inne | W pełni kompatybilne z zakupywanymi przełącznikami dystrybucyjnymi. |
| **Napęd taśmowy z taśmami** | | |
|  | Obudowa | Obudowa przeznaczona do montażu w szafie przemysłowej 19”. Wysokość biblioteki nie może przekraczać 2U. |
|  | Obsługiwane napędy | Obsługa napędów LTO-5, LTO-6, LTO-7 oraz LTO-8. |
|  | Zainstalowane napędy | Biblioteka taśmowa musi być wyposażona w 1 napęd LTO-8 o wydajności co najmniej 300MB/s oraz pojemności pojedynczej taśmy co najmniej 12TB – parametry podane bez kompresji danych. Interfejs napędu SAS.  Zaoferowana konfiguracja musi zawierać miejsce na instalację w przyszłości minimum 1 dodatkowego napędu taśmowego. |
|  | Sposób pracy napędu | Napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie co najmniej 100-300MB/s. |
|  | Zabezpieczenie danych | Obsługa sprzętowego szyfrowania danych w standardzie AES 256-bit dla wszystkich obsługiwanych typów napędów taśmowych.  Sprzętowe rozwiązanie (np. klucz USB lub dedykowane urządzenie) umożliwiające przechowywanie kluczy szyfrujących w sposób redundantny (dwie niezależne kopie kluczy). |
|  | Liczba slotów na kasety | Oferowana biblioteka musi być wyposażona w co najmniej 24 sloty na taśmy magnetyczne. |
|  | Sposób obsługi wymiany taśm w bibliotece | Oferowana biblioteka taśmowa musi posiadać możliwość konfiguracji tzw. „mail slot” umożliwiającego wymianę taśm bez konieczności wyjmowania z biblioteki całego magazynka z taśmami. |
|  | Dodatkowe funkcjonalności | Możliwość stosowania taśm typu WORM.  Mechanizm automatycznego czyszczenia głowic, brak konieczności cyklicznej obsługi konserwacyjnej przez personel techniczny.  Oferowana biblioteka musi być wyposażona w czytnik kodów kreskowych. |
|  | Taśmy | 24 taśmy LTO-7 RW z nalepkami z kodami kreskowymi. |
|  | Oprogramowanie zarządzające | Oferowana biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.  Oferowana biblioteka musi być wyposażona w oprogramowanie umożliwiające aktywne monitorowanie oraz analizę wydajności, utylizacji i stanu napędów taśmowych i nośników.  Wsparcie dla protokołu SNMP.  Jeśli powyższe funkcjonalności wymagają dodatkowych licencji, należy je dostarczyć wraz z urządzeniem. |
|  | Okablowanie | Do urządzenia należy dołączyć kable połączeniowe zgodnie z ilością i rodzajem zainstalowanych modułów. |
|  | Niezawodność | Parametr MSBF (mean swaps between failures) o wartości 2 000 000 dla pełnych cykli „załaduj/wyładuj”.  Parametr MTBF (mean time between failures) o wartości 100 000 godzin. |
| **Tablety medyczne – typ 1** | | |
|  | Ekran | Wielodotykowy  Typ IPS z podświetleniem LED  Rozdzielczość natywna nie mniejsza niż 800x480 pikseli  Przekątna ekranu od 5 do 6 cali  Jasność co najmniej 350 nitów |
|  | Procesor | Co najmniej 1,3Ghz |
|  | Obudowa | Posiadająca normę szczelności co najmniej IP54  Powłoka dezynfekowalna roztworem z zawartością alkoholu  Wytrzymująca upadek z min. 90 cm |
|  | Pamięć RAM | Co najmniej 1GB |
|  | Pamięć wewnętrzna | Co najmniej 16GB  Możliwość rozszerzenia pamięci kartą typu MicroSD SDHC do 32GB |
|  | Czas pracy na baterii | Co najmniej 6 godz. |
|  | Komunikacja | Wireless 802.11 a/b/g/n (2,4GHz I 5GHz)  Bluetooth 4.0 + EDR  HF RFID  NFC |
|  | Czytnik kodów kreskowych | Wbudowany w urządzenie czytnik kodów kreskowych 1D i 2D |
|  | Wejście komputerowe | Port ładowania i/lub multimedialny  Mini Jack 3.5 mm |
|  | Temperatura pracy | Nie więcej nić -10 do nie mniej niż +45 |
|  | System operacyjny | Android w wersji co najmniej 4.2 |
|  | Kamera | Przednia co najmniej 1.0Mp  Tylna co najmniej 5.0Mp |
|  | Inne | * Mikrofon, głośniki * Programowalne przyciski * Waga nie większa niż 350g * Stacja dokująca dedykowana pod zamawiany tablet umożliwiająca jego ładowanie * Możliwość dezynfekcji stacji dokującej roztworem z zawartością alkoholu   Wymaganie gwarancji producenta na min. 36 miesięcy. |
| **Tablety medyczne – typ 2** | | |
|  | Typ | Komputer przenośny typu tablet z ekranem min 8 max 13" |
|  | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb pracy lekarza, musi umożliwiać pracę w sterylnych pomieszczeniach. |
|  | Obudowa | Wodoszczelna, z powłoką antybakteryjną. IP67.  Musi posiadać gniazdo pamięci MicroSD. |
|  | Ekran | Ekran Wielodotykowy, min. (1280x800 pikseli)  Jasność ekranu minimum 600 nit (cd/m2) |
|  | Procesor | Min. Procesor 2 rdzeniowy, minimum 1,50 GHz |
|  | Pamięć operacyjna RAM | Min.1 GB |
|  | Parametry pamięci masowej | Min. 16 GB |
| 8. | Wyposażenie multimedialne | Zintegrowana kamera przednia i tylna, gniazdo 3,5mm z zintegrowanym wejściem na mikrofon |
|  | Wymagania dotyczące baterii i zasilania | Bateria typu hot-swap  Akumulator litowo-jonowy o pojemności min 6500 mAh |
|  | Waga i wymiary | Waga max 1,25 kg |
|  | System operacyjny | Zainstalowany system operacyjny w polskiej wersji językowej  Dopuszcza się rozwiązanie równoważne systemu operacyjnego o poniższych wymaganiach równoważności:  1) System w polskiej wersji językowej.  2) System wykorzystujący architekturę 64bit.  3) Pomoc systemowa dostępna w całości w języku polskim. |
|  | Wymagania dodatkowe | Odporność na upadek potwierdzona certyfikatem MIL-STD-810G  Zintegrowany czytnik kodów 1D/2D  Tablet musi umożliwiać weryfikację i autoryzację pracowników służby zdrowia zbliżeniowo - dzięki technologii NFC lub przez czytnik kart chipowych - Smart Card  Zintegrowane WiFi, Bluetooth® 4.0 i moduł WWAN minimum 3G.  Dokument potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych. |
|  | Inne | Współpracujące z oprogramowanie firmy NexusPolska – mObchód. |
| **Laptop** | | |
|  | Procesor | Procesor klasy x86–64/x64 co najmniej cztero-rdzeniowy, dedykowany do pracy w komputerach stacjonarnych. Taktowany zegarem co najmniej 3,9GHz oraz przynajmniej 6MB pamięcią L3 lub procesor równoważny. Zaoferowany procesor musi uzyskiwać w teście Passmark CPU Mark  średni (Average CPU Mark) wynik min. 8987 punktów (wynik zaproponowanego procesora musi znajdować się na stronie [www.cpubenchmark.net](http://www.cpubenchmark.net) **z dnia** **06.11.2019**) |
|  | Matryca | Niedotykowa matryca 14”, natywna rozdzielczość WQHD (2560x1440), format ekranu 16: 9, współczynnik kontrastu dynamicznego min 700:1, wbudowana kamera HD720p |
|  | System operacyjny Np. Windows 10 Pro lub równoważny (64 bitowy) wg. wskazanych obok funkcji i cech produktu równoważnego | 1. Preinstalowany, z oryginalnym nośnikiem instalacyjnym. 2. System operacyjny umożliwiający poprawne działanie oprogramowania systemu CliniNet, Eskulap, KS-SOMED oraz podłączenie do domeny Active Directory. 3. Dostarczona licencja ma być zbiorcza (OPEN/MOLP). |
|  | Pamięć systemowa | Minimum: 16 GB w standardzie DDR4 |
|  | Bateria (minimalnie) | Pozwoli na ciągłą pracę przez 16h na jednym naładowaniu; 50Wh |
|  | Waga (maksymalnie) | 1,5 kg |
|  | Wymiary (maksymalne) | 1. Szerokość:33 cm, 2. Głębokość:,23 cm 3. Wysokość: 20mm |
|  | Dźwięk | Wbudowane głośniki audio, jakości High Definition Audio oraz podwójny mikrofon |
|  | Rodzaje wejść / wyjść  (minimalnie) | 1. 2x USB 3.1 Gen 1 (one Always On), 2. 1x USB 3.1 Type-C Gen 1, 3. 1x USB 3.1 Type-C Gen 2 / Thunderbolt 3, 4. HDMI 1.4b, 5. Ethernet (RJ-45), 6. headphone / microphone combo jack, 7. side docking connector |
|  | Czytnik kart | Micro SD card reader |
|  | Karta graficzna (minimalne) | Częstotliwość rdzenia 300-1050MHz, Obsługuje pamięć DDR3/DDR3, obsługuję bibliotekę DirectX 12 |
|  | Dysk twardy | Pojemność: minimum 512GB SSD |
|  | Komunikacja | Wi-Fi 2x2 802.11ac + Bluetooth 5.0 |
|  | Nawigacja | Podświetlana klawiatura, TouchPad + TrackPoint |
|  | Bezpieczeństwo | 1. Możliwość zabezpieczenia poprzez: 2. Power-on password, 3. hard disk password, 4. supervisor password, 5. security keyhole, 6. dTPM 2.0, 7. Touch fingerprint reader 8. Laptop musi umożliwiać weryfikację i autoryzację pracowników służby zdrowia zbliżeniowo - dzięki technologii NFC lub przez czytnik kart chipowych - Smart Card” |
| **Punkt dostępowy Wifi** | | |
|  | Prędkość /transfer danych przez Ethernet LAN | 10,100,1000  Mbit/s |
|  | Maksymalny transfer danych przez bezprzewodowy LAN | 1300  Mbit/s |
|  | Maksymalna szybkość przesyłania danych | 1300  Mbit/s |
|  | Maksymalny zakres wewnętrzny (pomieszczenie) | 122  m |
|  | Przycisk reset | Tak |
|  | Certyfikaty | CE, FCC, IC |
|  | Ilość portów Ethernet LAN (RJ-45) | 2 |
|  | Liczba portów USB 2.0 | 1 |
|  | Poziom wzmocnienia anteny (max) | Każdy z modułów radiowych musi posiadać trzy wewnętrzne,  zintegrowane, dookólne anteny o zysku energetycznym  a) 22 dBm dla 2.4 GHz,  b) 22 dBm dla 5 GHz |
|  | Ilość anten | 3 |
|  | Zasilanie | Wymagane jest, aby zasilanie urządzenia było zrealizowane za  pośrednictwem 802.3af PoE lub 802.3at PoE+ |
|  | Szyfrowanie transmisji bezprzewodowych | WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES) |
|  | Pasmo pracy | 2,4GHz oraz 5GHz |
|  | Architektura | Wymagane jest dostarczenie skalowalnego, inteligentnego systemu  dostępu bezprzewodowego.  System musi pracować w architekturze gwarantującej centralne  zarządzanie i kontrolowanie punktów dostępowych AP (access points). Całość konfiguracji odbywać się w konsoli centralnej (kontroler)  i następnie ma być automatycznie propagowana na punkty dostępowe.  Dostarczony kontroler musi obsługiwać minimum 25 urządzeń |
|  | Zarządzanie transmisją | 802.1Q, QoS, tryb Hotspot, portal dla gości, Izolacja ruchu gości, MultiSSID (minimum 3 jednocześnie) |
|  | Inne | Możliwość montażu na ścianie lub pod sufitem |
|  | Zestaw montażowy | Punkt dostępowy zostanie dostarczony z uchwytem umożliwiającym  instalację naścienną/sufitową. |
| **Terminal komputerowy** | | |
|  | Procesor | Procesor klasy x5 czterordzeniowy taktowany zegarem minimum 1,44 GHz |
|  | Karta graficzna,  Łącza karty graficznej | Zintegrowana obsługująca rozdzielczość do 2560 x 1600, 60Hz  2 x DisplayPort |
|  | Ilość pamięci RAM | 2 GB DDR3 1600 MHz |
|  | Pamięć Flash | Min 16 GB |
|  | Złącza na tylnym panelu | 1. 1 x RJ45 2. 2 x USB |
|  | Złącza na przednim panelu | 1. 1 x USB 2.0 2. 1 x USB 3.0 3. Audio |
|  | Wymiary | Nie większe niż 19cmx7cmx19cm |
|  | Waga całkowita | Nie więcej niż 1,53Kg |
|  | Karta sieciowa | 10 /100/1000 |
|  | Zgodność | Pełna zgodność z Citrix XenDesktop, Microsoft RDS i VMware Horizon. |
| **Komputer stacjonarny z monitorem i oprogramowaniem** | | |
|  | Taktowanie procesora | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 8000 punktów, załączyć do oferty wyniki przeprowadzonego testu |
|  | Dysk | 256 GB SDD |
|  | Napęd optyczny | TAK DVD-RW |
|  | Zainstalowana pamięć RAM | 8 GB; Rodzaj Pamięci DDR4 |
|  | Częstotliwość szyny pamięci | 2666 MHz |
|  | Maks. wielkość pamięci | 32 GB |
|  | Porty USB | 4 x USB 2.0 Type-A, 4 x USB 3.0 Type-A |
|  | Porty wideo | 1 x DisplayPort, 1 x VGA (15 pin D-Sub) |
|  | Pozostałe porty we/wy | 1 x Audio (Line-in), 1 x Audio (Combo), 1 x Audio (Line-out), 1 x RJ-45 |
|  | Akcesoria w zestawie | 1. Klawiatura z czytnikiem kart Smartcard 2. Mysz optyczna |
|  | Przekątna monitora | 21.5 cali,plamka 0,27mm, Jasność 250cd/m2, kąty widzenia 178/178 stopni, czas reakcji matrycy max 8ms, |
|  | Rozdzielczość nominalna monitora | [1920 x 1080 (Full HD) piksele](https://www.komputronik.pl/search-filter/1251/monitory-full-hd), , częstotliwość odświeżania poziomego 30-83kHz, Pionowego 56-76Hz,, powłoko anty odblaskowa, podświetlenie LED, zakres regilacji Kąta min -5 do +21 stopni |
|  | Porty wejścia/wyjścia monitora | 1. [1 x HDMI](https://www.komputronik.pl/search-filter/1251/monitory-hdmi) 2. 1 x D-Sub 15-pin 3. 1 x DisplayPort 4. 3 x USB 3.0 5. Wbudowane głośniki stereo min 2W |
|  | Zgodność z technologią HDCP | Tak |
|  | Akcesoria | 1. Przewód zasilania 2. Przewód VGA 3. Kabel USB (wtyczka męska typu A do wtyczki męskiej typu B) 4. Kabel DisplayPort™ 1.2 zgodny z zestawem 5. Instrukcja użytkownika, sterowniki 6. HP Display Assistant |
|  | Akcesoria | Kabel DisplayPort |
|  | Oprogramowanie | Office Home and Business 2019 PL EuroZone Medialess lub równoważne:  Warunki równoważności:   1. Pełna polska wersja językowa interfejsu użytkownika; 2. Wbudowany system pomocy w języku polskim; 3. Możliwość dokonywania aktualizacji i poprawek oprogramowania przez Internet z możliwością wyboru instalowanych poprawek; 4. Darmowe aktualizacje oprogramowania przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW producenta systemu; 5. Internetowa aktualizacja zapewniona w języku polskim; 6. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. 7. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 8. Edytor tekstów, 9. Arkusz kalkulacyjny, 10. Narzędzie do przygotowywania i prowadzenia prezentacji, 11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, 12. kalendarzem, kontaktami i zadaniami. 13. Edytor tekstów musi umożliwiać: 14. 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, 15. Wstawianie oraz formatowanie tabel, 16. Wstawianie oraz formatowanie obiektów graficznych, 17. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), 18. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, 19. Automatyczne tworzenie spisów treści, 20. Formatowanie nagłówków i stopek stron, 21. Sprawdzanie pisowni w języku polskim, 22. Śledzenie zmian wprowadzonych przez użytkowników, 23. Wydruk dokumentów, 24. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, 25. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007,2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. Zapewnienie po edycji i zapisaniu danego dokumentu bezproblemową jego dalszą pracę w programach Microsoft Word 2003, 2007, 2010, 2013 i 2016, 26. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 27. Arkusz kalkulacyjny musi umożliwiać: 28. Tworzenie raportów tabelarycznych, 29. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, 30. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, 31. Tworzenie raportów z zewnętrznych źródeł danych np.: inne arkusze kalkulacyjne, 32. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, 33. Wyszukiwanie i zamianę danych, 34. Wykonywanie analiz danych przy użyciu formatowania warunkowego, 35. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, 36. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, 37. Formatowanie czasu, daty i wartości finansowych z polskim formatem, 38. Zapis wielu arkuszy kalkulacyjnych w jednym pliku, 39. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. Zapewnienie po edycji i zapisaniu danego dokumentu bezproblemową jego dalszą pracę w programach Microsoft Excel 2003, 2007, 2010, 2013 i 2016, 40. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 41. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: 42. Prezentowanie przy użyciu projektora multimedialnego, 43. Drukowanie w formacie umożliwiającym robienie notatek, 44. Zapisanie jako prezentacja tylko do odczytu, 45. Nagrywanie narracji i dołączanie jej do prezentacji, 46. Opatrywanie slajdów notatkami dla prezentera, 47. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, 48. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, 49. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, 50. Możliwość tworzenia animacji obiektów i całych slajdów, 51. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, 52. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007, 2010, 2013 i 2016. Zapewnienie po edycji i zapisaniu danego dokumentu bezproblemową jego dalszą pracę w programach Microsoft PowerPoint 2003, 2007, 2010, 2013 i 2016. 53. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: 54. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, 55. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, 56. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, 57. Automatyczne grupowanie poczty o tym samym tytule, 58. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, 59. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, 60. Zarządzanie kalendarzem, 61. Udostępnianie kalendarza innym użytkownikom, 62. Przeglądanie kalendarza innych użytkowników, 63. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, 64. Zarządzanie listą zadań, 65. Zlecanie zadań innym użytkownikom, 66. Zarządzanie listą kontaktów, 67. Udostępnianie listy kontaktów innym użytkownikom, 68. Przeglądanie listy kontaktów innych użytkowników, 69. Możliwość przesyłania kontaktów innym użytkowników     W szczególności Wykonawca musi zapewnić stabilność i pełną wymaganą funkcjonalność współpracy z posiadanym przez Zamawiającego następującym oprogramowaniem:   1. pełną zgodność z formatami plików utworzonych za pomocą oprogramowania MS Office 2003, 2007, 2010, 2013 i 2016. Zapewnienie po edycji i zapisaniu danego dokumentu bezproblemową jego dalszą pracę w programach Microsoft 2003, 2007, 2010, 2013 i 2016, 2. ciągłości pracy w menedżerze poczty elektronicznej oraz informacji (konieczność migracji obecnych wiadomości, zadań, kontaktów, informacji i kalendarza spotkań do nowego programu). |
| **Duplikator Płyt DVD** | | |
|  | Specyfikacja duplikatora | 1. Autonomiczne urządzenie do automatycznej duplikacji płyt CD/DVD ( bez konieczności użycia komputera). Sterowane bezpośrednio z klawiatury urządzenia. 2. Szybkość odczytu - min 48x CD, 16x DVD. 3. Szybkość kopiowania - min 40x CD, 8x DVD. 4. Obsługiwane formaty płyt: CDROM, Audio CD, VideoCD, PhotoCD, CDROM/XA, CD-DA, DVD-/+R, DVD-/+RW, DVD DL, Multisession. 5. Możliwość rozbudowy o dysk twardy. 6. Wyświetlacz - informujący o stanie operacji. 7. Zasilanie – 230V. Waga - do 8kg. |
|  | Inne | Współpraca z modułami RIS/PACS systemu HIS Eskulap |
| **Czytnik kodów kreskowych** | | |
|  | Rodzaje interfejsu | Multiinterfejs USB, KBW (PS/2), RS232 |
|  | Typ skanera: | 2D, imager |
|  | Odczytywane kody kreskowe | 1D: Code 39, Code 128, Code 93, Codabar/NW7, Code 11, MSI Plessey, UPC/EAN, I 2 of 5, Korean 3 of 5, GS1 DataBar, Base 32 (Italian Pharma) 2D: PDF417, Micro PDF417, Composite Codes, TLC-39, Aztec, DataMatrix, MaxiCode, QR Code, Micro QR, Chinese Sensible (Han Xin), Postal Codes |
|  | Maksymalny zasięg odczytu | Co najmniej 36 cm |
|  | Tolerancja ruchu | 13cm/s |
|  | Sygnalizacja odczytu | Dźwiękowa i świetlna |
|  | Odporność na upadki | Co najmniej z wysokości 1,5 m |
|  | Norma szczelności | IP42 zgodnie z normą PN-EN 60529:2003 lub równoważną w zakresie oznaczania stopni ochrony zapewnianej przez obudowy przed dostępem do części niebezpiecznych, wnikaniem obcych ciał stałych, wnikaniem wody oraz system podawania dodatkowych informacji związanych z taką ochroną |
|  | Zasięg pracy od bazy komunikacyjno-ładującej | 10 m |
|  | Temperatura otoczenia pracy | Od 0 st. C do 50 st. C |
|  | Wilgotność otoczenia pracy | Od 5% do 95% |
|  | Waga | do 420 g |
|  | W komplecie | Czytnik, instrukcja obsługi |
| **Drukarka kodów kreskowych** | | |
|  | Specyfikacja | 1. Rodzaj Druku: Termotransfer 2. Rozdzielczość Drukowania: 203dpi 3. Maksymalna Szerokość Druku: 104mm 4. Maksymalna Długość Druku: 991mm 5. Maksymalna Prędkość Druku: 127mm/s 6. Maks. Długość Taśmy: 74 metry 7. Pamięć Ram: 8 MB 8. Pamięć Flash: 4 MB 9. Interfejs USB: Tak 10. Interfejs Ethernet: TAK 11. Interfejs RS232: NIE 12. Połączenie Bezprzewodowe: Brak 13. Języki Programowania: EPLII, ZPLII, XML 14. Dyspenser (Odklejak): Nie 15. Gilotyna (Nóż): Nie 16. Ekran: Brak 17. Oprogramowanie w Zestawie: Projektowanie Etykiet 18. Taśma Termotransferowa: Na Rolce |
| **Urządzenia wielofunkcyjne - typ 1** | | |
|  | Dane ogólne | 1. Prędkość drukowania i kopiowania: Do 40 stron A4 na minutę, do 21 stron A3 na minutę 2. Rozdzielczość drukowania: 1200 x 1200 dpi, 3. Rozdzielczość skanowanie/kopiowanie: 600 x 600 dpi 4. Czas nagrzewania: maksymalnie 20 sek. od włączenia zasilania 5. Czas pierwszego wydruku: nie większy niż 4,5 sek. 6. Czas pierwszej kopii: 5 sek. lub mniej (DP), 7. Wymiary (szer x gł x wys) nie większe niż: 594 x 696 x 683 mm 8. Waga: max 60 kg 9. Pobór mocy    1. Drukowanie nie więcej niż: 600 W,    2. Tryb gotowości nie więcej niż: 100 W,    3. Tryb oszczędzania energii nie więcej niż: 4,0 W 10. Napięcie zasilania: AC 220 V ~ 240 V, 50/60 Hz 11. Poziom hałasu zgodnie z normą ISO 7779 Drukowanie/kopiowanie: 67 dB(A) LpA, tryb gotowości: 43 dB(A) LpA 12. Pamięć Standard 2048 MB, 8 GB SSD + standard 320 GB HDD |
|  | Drukowanie | 1. Emulacje PCL6 (PCL5c / PCL-XL), KPDL3 (zgodna z PostScript 3), bezpośrednie drukowanie PDF, bezpośrednie drukowanie XPS, PPML 2. Minimum 80 czcionek PCL |
|  | Kopiowanie | 1. Zakres zoom 25 - 400 % co 1% 2. Kopiowanie ciągłe 1 - 999 3. Ustawienia obrazu Tekst, Zdjęcie, Tekst + Zdjęcie, Grafika/Mapa, Wydrukowany dokument |
|  | Skanowanie | 1. Typ pliku: TIFF, PDF, PDF/A, JPEG, Open XPS, szyfrowany PDF, wysoko skompresowany PDF, PDF/A-1a/b, PDF/A-2a/b/u 2. Funkcje: kolorowy skan, wewnętrzna książka adresowa, obsługa Active Directory, szyfrowana transmisja danych, wysyłanie do kilku miejsc jednocześnie (e-mail, faks, SMB/FTP folder, druk), pomijanie pustych stron 3. Rozpoznawanie oryginału: Tekst + Zdjęcie, Zdjęcie, Tekst, Light Tekst, Tekst (zoptymalizowany pod OCR) 4. Funkcjonalności skanera: Skan do e-mail, do FTP, do SMB, do USB Host, skan do skrzynki, TWAIN (network), WIA, WSD 5. Dostępne rozdzielczości: 600 x 600 dpi, 400 x 400 dpi, 300 x 300 dpi, 200 x 400 dpi, 200 x 200 dpi, 200 x 100 dpi (24 bit), (256 odcieni szarości) 6. Szybkość skanowania: (A4, 300 dpi, Dual Scan z DP-7110/DP-7100) 80 obrazów na minutę mono, 80 obrazów na minutę kolor |
|  | Funkcje dodatkowe | 1. Skanowanie Elektronicznej Dokumentacji Medycznej musi odbywać się za pomocą jednej aplikacji zainstalowanej na urządzeniu wielofunkcyjnym. 2. Aplikacja musi umożliwiać tworzenie Elektronicznej Dokumentacji Medycznej przy wykorzystaniu ekranu dotykowego urządzenia wielofunkcyjnego. 3. Aplikacja musi umożliwiać zalogowanie się do systemu HIS Eskulap za pomocą loginu i hasła i wprowadzenie EDM zautoryzowanemu użytkownikowi. 4. Aplikacja musi umożliwiać wybór pacjenta poprzez wprowadzenie numeru PESEL i wybór typu skanowanego dokumentu oraz przesłanie go do systemu. |
|  | Wymagania dodatkowe | 1. Oferent musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia wielofunkcyjnego - dokumenty potwierdzające należy dołączyć do oferty. 2. Certyfikat ISO 9001:2015 producenta oferowanego sprzętu - dokument potwierdzający należy załączyć do oferty. 3. Certyfikat ISO 14001:2015 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty. 4. Oświadczenie producenta oferowanego sprzętu lub jego autoryzowanego przedstawiciela w Polsce, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Konieczność nie zachodzi w przypadku autoryzowanego przedstawiciela producenta. |
| **Urządzenia wielofunkcyjne - typ 2** | | |
|  | Dane ogólne | 1. Rozdzielczość - drukowanie: 1200 x 1200 dpi, 2. Rozdzielczość - skanowanie/kopiowanie: 600 x 600 dpi 3. Czas nagrzewania: maksymalnie 25 sek. 4. Czas pierwszego wydruku: maksymalnie 5 sek. 5. Czas pierwszej kopii: maksymalnie 6 sek. 6. Waga max 24 kg 7. Pobór mocy    1. Drukowanie nie więcej niż : 730 W,    2. Tryb gotowości nie więcej niż: 75 W,    3. Tryb oszczędzania energii nie więcej niż: 5 W 8. Napięcie zasilania: AC 220 V ~ 240 V, 50/60 Hz 9. Poziom hałasu zgodnie z normą ISO 7779 10. Drukowanie/kopiowanie: max. 56 dB(A) LpA, tryb gotowości: 30 dB(A) LpA 11. Pamięć Standard 1GB Max. 3GB + 128GB SSD |
|  | Drukowanie | 1. Emulacje PCL6 (5c/XL), KPDL3 (PostScript 3), bezpośrednie drukowanie PDF oraz XPS, wsparcie AES, TIFF/JPEG Direct Print Support, Open XPS, Line Printer, IBM Proprinter X24E, Epson LQ-850 2. Minimum 80 czcionek PCL |
|  | Kopiowanie | 1. Zakres zoom 25 - 400 % co 1% 2. Kopiowanie ciągłe 1 - 999 3. Ustawienia obrazu Tekst, Zdjęcie, Tekst + Zdjęcie, Grafika/Mapa, Wydrukowany dokument |
|  | Skanowanie | 1. Szybkość skanowania 60 obrazów na minutę (300 dpi, A4, mono) 40 obrazów na minutę (300 dpi, A4 kolor) 26 obrazów na minutę (300 dpi, A4, mono, dupleks) 17 obrazów na minutę (300 dpi, A4, kolor, dupleks) 2. Dostępne rozdzielczości 600, 400, 300, 200 dpi (256 odcieni szarości) 3. Tryby skanowania Skan do e-mail, skan do FTP, do SMB, do USB Host, Network TWAIN, WSD 4. Typ pliku TIFF, JPEG, XPS, Open XPS, PDF, PDF/A, PDF/A-1a/b, PDF/A-2a/b/u, szyfrowany PDF, wysoko skompresowany PDF PDF, MS Office, przeszukiwalny PDF (opcjonalnie wymagany Scan Extension Kit(A)) 5. Rozpoznawanie oryginału Tekst, zdjęcie, tekst + zdjęcie, Tekst (zoptymalizowany pod OCR) |
|  | Funkcje dodatkowe | 1. Skanowanie Elektronicznej Dokumentacji Medycznej musi odbywać się za pomocą jednej aplikacji zainstalowanej na urządzeniu wielofunkcyjnym. 2. Aplikacja musi umożliwiać tworzenie Elektronicznej Dokumentacji Medycznej przy wykorzystaniu ekranu dotykowego urządzenia wielofunkcyjnego. 3. Aplikacja musi umożliwiać zalogowanie się do systemu HIS Eskulap za pomocą loginu i hasła i wprowadzenie EDM zautoryzowanemu użytkownikowi. 4. Aplikacja musi umożliwiać wybór pacjenta poprzez wprowadzenie numeru PESEL i wybór typu skanowanego dokumentu oraz przesłanie go do systemu. |
|  | Wymagania dodatkowe | 1. Podmiot serwisujący musi posiadać wdrożony system zarządzania jakością zgodny z ISO 9001:2015 lub równoważną w zakresie świadczenia usług serwisowych oraz posiadać autoryzację producenta urządzenia wielofunkcyjnego - dokumenty potwierdzające należy dołączyć do oferty. 2. Certyfikat ISO 9001:2015 lub równoważny producenta oferowanego sprzętu - dokument potwierdzający należy załączyć do oferty. 3. Certyfikat ISO 14001:2015 lub równoważny producenta oferowanego sprzętu - dokument potwierdzający należy załączyć do oferty. 4. Oświadczenie producenta oferowanego sprzętu lub jego autoryzowanego przedstawiciela w Polsce, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z gwarancją. Konieczność złożenia oświadczenia nie zachodzi w przypadku autoryzowanego przedstawiciela producenta. |
| **UTM** | | |
|  |  | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. System bezpieczeństwa UTM musi zostać dostarczony w klastrze wysokiej dostępności co najmniej Active-Passive.  Dla dostarczonych elementów systemów bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:   1. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. 2. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. Dopuszcza się system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej z wykluczeniem platform sprzętowych lub programowych, które wysyłają logi do chmury zlokalizowanej poza terenem Unii Europejskiej. 3. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:    1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection    2. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla co najmniej plików typu: rar, zip.    3. Poufność danych - IPSec VPN oraz SSL VPN    4. Ochrona przed atakami - Intrusion Prevention System (IPS/IDS)    5. Kontrola stron Internetowych – Web Filter    6. Kontrola zawartości poczty – antyspam (dla protokołów SMTP, POP3)    7. Kontrola pasma oraz ruchu (QoS i Traffic shaping)    8. Kontrola aplikacji oraz rozpoznawanie ruchu P2P    9. Analiza ruchu szyfrowanego protokołem SSL 4. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:    1. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site    2. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem    3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności    4. Praca w topologii Hub and Spoke oraz Mesh    5. Obsługa mechanizmów: IPSec    6. Obsługa ssl vpn w trybach portal oraz tunel 5. Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. 6. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. 7. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety). 8. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 9. Sygnatury AV muszą być weryfikowane i udostępniane na serwerach producenta systemu bezpieczeństwa. 10. Oferowany system bezpieczeństwa nie może wysyłać plików poza teren Unii Europejskiej, pliki nie mogą być też udostępniane innym podmiotom. 11. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1500 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS. 12. Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 13. Baza filtra WWW pogrupowana w minimum 60 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. 14. Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. 15. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników 16. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. 17. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów. 18. W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:     1. Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego. 19. System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania. 20. Oferowany system bezpieczeństwa po zakończeniu trwania licencji nie może zablokować pracujących na nim modułów bezpieczeństwa. System będzie pracował na sygnaturach i regułach pobranych w ostatnim dniu aktywnej licencji. 21. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ dla rozwiązań kategorii Network Firewall. 22. Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 23. Interfejsy 10/100/1 000 8-16 24. Światłowód 1 GB lub 10 GB (opcja) 25. Pamięć wewnętrzna 320 GB 26. Przepustowość IPSec min 2400 27. Maks. liczba tuneli IPSec min 1000 28. Maks. liczba tuneli SSL min 150 29. Liczba jednoczesnych sesji 1000000 30. Nowe sesje / sekundę 40000 31. 802.1Q VLAN (max) 256 32. Firewall 10Gbps. |
| **Szafa serwerowa** | | |
|  | Wymagania ogólne | Dostarczyć należy wyposażoną szafę typu Rack 47U (przeznaczoną do instalacji i eksploatacji sprzętu IT). Wewnątrz szafy zainstalowana musi być jednostka klimatyzacji w oparciu o instalację DX – bezpośrednie odparowanie z zewnętrznym skraplaczem.  W celu zapewnienia najwyższego stopnia wymaganej bezawaryjności, dostępności, wydajności i efektywności energetycznej, skalowalności całości budowanego układu oraz najwyższego stopnia bezpieczeństwa pracy powinny zostać zastosowane wszystkie wymienione niżej urządzenia produkowane przez jednego producenta:   1. urządzenia chłodnicze, parowniki, zintegrowane w szafie 19” w układzie zamkniętym, chłodzenie w sposób neutralny dla temp. powietrza w pomieszczeniu, 2. skraplacze zewnętrzne, 3. szafy 19” IT, 4. urządzenia gaśnicze wraz z wczesną detekcją pożaru, 5. system zdalnego monitoringu warunków środowiskowych. |
|  | Urządzenia chłodnicze zintegrowane w szafie 19” IT | 1. Klimatyzator typu split DX o mocy 6,5 kW składający się z jednostki wewnętrznej (parownik) i jednej jednostki zewnętrznej (chłodziarki z regulacją inwerterową). 2. Konstrukcja jednostki wewnętrznej umożliwiająca zainstalowanie w szafie IT o szerokości 800 mm, montowana wewnątrz szafy IT pomiędzy ramą 19” a ścianą boczną szafy IT.  Konstrukcja zoptymalizowana pod kątem IT w taki sposób, aby idealnie wspomagać prowadzenie powietrza „Front to Back“ zabudowy 19". Jednostka wewnętrzna zasysająca ciepłe powietrze wylotowe z serwerów bezpośrednio w tylnej części szafy a schłodzone wydmuchiwane po bokach przed płaszczyzną 19". Obudowa jednostki wewnętrznej wykonana z blachy stalowej powlekanej proszkowo, wewnątrz parownik bezpośredni, 4 wentylatory promieniowe EC, kolektor i odpływ kondensatu. 3. Urządzenia powinno pozwalać na montaż z lewej lub z prawej strony szafy serwerowej IT. Jednostka wewnętrzna powinna być wyposażona w sterownik mikroprocesorowy do regulacji temperatury powietrza na wlocie do serwera. Zakres nastawy temperatury wlotowej na serwer to przedział od 20°C do 28°C. 4. Wchodzący w skład systemu zewnętrzny czujnik powinien być umieszczony przed serwerem.  Jednostka zewnętrzna ze sprężarką powinna posiadać regulację inwerterową umożliwiającą bezstopniowe dopasowanie mocy także podczas pracy w trybie obciążenia częściowego. Połączenie między jednostką wewnętrzną a zewnętrzną powinno odbywać się za pomocą rurek miedzianych, przewodu danych i zasilania elektrycznego.  Urządzenie wewnętrzne zasilane przez napięcie z urządzenia zewnętrznego. 5. Jako czynnik chłodniczy powinien zostać zastosowany R410a.   **Dane techniczne:**   1. Użytkowa moc chłodnicza maksymalnie 6,5 kW 2. Zainstalowane wentylatory w jednostce wewnętrznej: 4 3. Podstawa regulacji: temperatura powietrza na wlocie do serwera, ustawiona na maksimum 22°C 4. Zasilanie elektryczne: 230V, 1~, N, PE, 50 Hz 5. Zabezpieczenie: 16A 6. Czynnik chłodniczy: R410a 7. Wymiary jednostki wewnętrznej, szer. x wys. x gł.: 105x1550x820 mm 8. Wymiary jednostki zewnętrznej, szer. x wys. x gł.: 845 x 700 x 320 mm 9. Dopuszczalne są różnice w wymiarach +/- 5mmMasa jednostki wewnętrznej: maksymalnie 48 kg 10. Masa jednostki zewnętrznej: maksymalnie 42 kg 11. Zakres temperatur otoczenia, jedn. zewn.: -20°C do +45°C |
|  | Szafa 19” serwerowa | 1. Integralną częścią systemu chłodzenia w technologii chłodzenia wymiennikiem chłodniczym Rackowym musi być szafa IT - 19”. Wymagane są szafy IT tego samego producenta co wymienników chłodniczych oraz skraplaczy tak, aby zapewniona została jak najwyższa dostępność, spójność rozwiązań i optymalizacja poprawnego działania elementów w całości dostarczonego systemu. 2. Należy dostarczyć szafę 19” IT o wymiarze 800mmx2200mmx1200mm (szerokość x wysokość x głębokość) każda. 3. Minimalne wymagania techniczne, funkcjonalne, wyposażenia dla szaf serwerowych, sieciowych: 4. Szafa IT dopuszczona przez producenta do klimatyzacji oraz wczesnego wykrywania i gaszenia pożaru tylko wewnątrz, dla układu zamkniętego, neutralny dla powietrza otoczenia serwerowni. 5. Szafa serwerowa, 19”, konstrukcja ramy szaf sztywna, spawana. 6. Wysokość zabudowy szaf serwerowych 47U, wraz z dodatkową separacją frontową strefy zimnej. 7. Przednie drzwi przeszklone o szczelności IP55 (szkło bezpieczne hartowane ESG 3mm), tylne drzwi dzielone pionowo z blachy stalowej pełne. Płyta dachu pełna. 8. Dwie płaszczyzny mocowania 482,6 mm (19“) z przodu i z tyłu na wspornikach montowanych po głębokości szafy w części dachowej oraz podłogowej ramy szafy. 9. Łączna obciążalność obu płaszczyzn montażowych 19” min. 1500 kg. Obciążalność szafy potwierdzona odpowiednim dokumentem. 10. Płaszczyzny montażowe 19” powinny składać się z uniwersalnych szyn profilowych do zastosowań serwerowych, sieciowych i elektronicznych, z bezstopniową regulacją głębokości, mocowanie do poprzeczek. Mocowanie szyn profilowych powinno odbywać się elastycznie, bez użycia narzędzi, za pomocą szybkozłączy. Szyny profilowe z przodu i z tyłu z dodatkowym otworowaniem w standardzie EIA 310 E. Wszystkie jednostki wysokości powinny być oznakowane na szynach profilowych i ponumerowane w przeciwnych kierunkach. Oznakowanie U obu płaszczyzn montażowych powinno być czytelne od przodu. Wszystkie poprzeczki ze zintegrowaną podziałką do szybkiego określania odstępów montażowych i pozostałej wolnej przestrzeni z przodu. 11. Szyny profilowe 19” z przodu muszą być przygotowane do beznarzędziowego montażu elementów ułatwiających prowadzenie kabli i organizowania struktury okablowania o maksymalnej gęstości upakowania. 12. Szyny profilowe 19” z tyłu muszą być przygotowane do obustronnego zamocowania Power Distribution Unit (PDU) o wymiarze 1U do zelektryfikowania szafy bez zużywania objętości pod zabudowę dzięki montażowi pomiędzy płaszczyzną montażową a ścianą boczną, w przestrzeni zero-U. Montaż PDU możliwy pod dwie PDU na każdą ze stron. 13. Szafa o szer. 800mm powinna mieć możliwość realizacji zabudowy 19" w standardzie jako centralna wypośrodkowana lub jako asymetryczna z możliwością przesuwania do skrajnego dowolnego boku szafy. Możliwość realizacji zabudowy profili pod sprzęt IT w standardzie: 19", 21", 23", 24" bez dodatkowych przeróbek mechanicznych, akcesoriów montażowych. 14. Akcesoria montażowe 19“ i kompletny zestaw uziemienia dołączone luzem do zestawu. 15. Szafę dodatkowo powinna być wyposażona od frontu szafy z mocowaniem do przedniego profilu 19-calowego w częściową pionową prowadnicę powietrza zabudowaną po przeciwnej stronie do wewnętrznego wymiennika DX. Prowadnica powinna posiadać panele zaślepiające 3 x1U - 19", dla dodatkowej pow. montażowej. 16. Materiał:  * Blacha stalowa, * Tworzywo sztuczne zgodne z UL 94-V0 * Powierzchnia: lakierowana.  1. Dla prowadzenia Kabli w pionie szafa musi być dodatkowo wyposażona w koryto montażowe kablowe pionowe, montowane po głębokości szafy na wydzielonym poziomie montażowym. Montaż możliwy bez użycia narzędzi . 2. Dla zaślepienia wolnej przestrzeni należy z szafą dostarczyć panele zaślepiające o wysokości min. 9U przeznaczone do beznarzędziowego montażu w 19”. Panele zaślepiające mają zapewnić odpowiednie prowadzenie powietrza oraz zapewnić właściwy sposób rozprowadzenia gazu gaśniczego. Każdy panel musi posiadać: odporność ogniową według UL 94 HB i być samogasnący, możliwość indywidualnego dopasowania wielkości przez wyłamanie wytłaczanych elementów 1U. 3. Dodatkowo szafa powinna zostać wyposażona w min. jeden poziomy panel porządkujący 1U wraz z pięcioma wieszakami stalowymi o wym. 43x105mm każdy. Szerokość: 482,6 mm (19"). 4. Materiał:  * Panel: blacha stalowa, * Wieszak: stal ocynkowana.  1. Szafa dostarczona musi zostać wraz z dwoma zintegrowanymi listwami zasilania PDU Metered, opomiarowane na każdą z faz z podłączeniem do sieci zdalnego monitorowania. Przewidziane powinny być dwa tory prądowe dla szafy. Listwy PDU muszą posiadać możliwość montażu w sposób beznarzędziowy w przestrzeni pomiędzy ścianą boczną a profilem 19” z dwoma bliźniaczymi listwami. Dla szafy powinna zostać zastosowana listwa PDU o max. prądzie 1x 32A. |
|  | Opis technologiczny PDU w wersji Metered | 1. Zakres napięcia wejściowego (L-N):90V – 260(400)V AC, 50-60Hz 2. Prąd wejściowy: 32A 3. Liczba faz: 1 4. Liczba gniazdek typu EN60320/C13 (łącznie): min. 24 5. Liczba gniazdek typu EN60320/C13 (na fazę / bezpiecznik): min. 12 6. Liczba gniazdek typu EN60320/C19 (łącznie): min 4 7. Liczba gniazdek typu EN60320/C19 (na fazę / bezpiecznik): min. 2 8. Liczba wyłączników ochronnych: min. 2 9. Liczba elektromagnetycznych wyłączników ochronnych: min. 16A Typ C 10. Wtyk przyłączeniowy wejścia PDU: EN60309 / CEE 11. Długość kabla przyłączeniowego: min. 3m 12. Typ kabla przyłączeniowego: H05-VV 13. Liczba żył: 3 14. Przekrój kabla: 4mm² 15. Szerokość max. obudowy PDU: 44mm (1 U) 16. Głębokość max. obudowy PDU: 70mm 17. Wysokość max. obudowy PDU: 1900mm 18. Materiał PDU: aluminium, anodowane, 19. Adapter mocujący PDU: tworzywo sztuczne, czarny 20. Funkcje pomiaru: Pomiar dla każdej fazy lub zasilania 21. Rejestrowane wartości (na fazę): Napięcie (V), prąd (A), częstotliwość (Hz),Moc czynna (kW), praca czynna (kWh), moc bierna (VA), praca bierna (kVAh), Współczynnik mocy (cos fi), Pomiar przewodu zerowego / określanie obciążenia asymetrycznego, Kontrola wkładki bezpiecznikowej (w wersjach 32A/63A) 22. Zakres pomiaru napięcia: 90V- 260V 23. Rozdzielczość pomiaru napięcia: 0,1V 24. Dokładność pomiaru napięcia: 2% 25. Zakres pomiaru prądu: 0–32A 26. Rozdzielczość pomiaru prądu: 0,1A 27. Dokładność pomiaru prądu: 2% 28. Dokładność pomiaru częstotliwości: 2% 29. Dokładność pomiaru mocy czynnej (kW): 2% 30. Dokładność pomiaru mocy pozornej (KVA): 2% 31. Dokładność pomiaru pracy czynnej (kWh): 1% 32. Dokładność pomiaru pracy biernej (kVAh): 2% 33. Dokładność pomiaru współczynnika mocy: 2% 34. Konfigurowalne wartości graniczne (ostrzeżenie/alarm): Tak 35. Licznik godzin pracy: Tak 36. Wyświetlacz / wskaźniki: OLED, RGB 128x128 pikseli 37. Interfejs sieciowy: RJ45, zintegrowany websewer 38. Obsługiwane protokoły: HTTP, HTTPS, SSL, SSH, NTP, Telnet TCP/IP v4 i v6, DHCP, DNS, NTP, Syslog, SNMP v1, v2c i v3, XMLFTP/SFTP (aktualizacja / transfer plików) Wysyłanie e-maili (SMTP) 39. Administrowanie użytkownikami i uprawnieniami: Tak 40. Integracja z LDAP(S)/Radius/Active Directory: Tak 41. Port USB do aktualizacji firmware i funkcji rejestrowania danych: Tak 42. Interfejs CAN-Bus: RJ45, do podłączania czujników 43. Typy czujników CAN: temperatura, temperatura i wilgotność (kombi), czujnik dostępu IR, czujnik wandalizmu 44. Mini. liczba czujników na 1 PDU: 4 45. Zgodność:CE 46. Bezpieczeństwo: PN-EN 60950-1 47. EMC: PN-EN 55022 / B,PN-EN 61000-4-2,PN-EN 61000-4-3,PN-EN 61000-6-2,PN-EN 61000-6-3 48. Dyrektywa bezpieczeństwa: 2014/35/EU 49. Dyrektywa EMC: 2014/30/EU 50. Stopień ochrony: IP 20 (PN-EN 60529 lub równoważna) 51. Klasa ochrony: Klasa 3 52. Stopień zabrudzenia: 2 53. Klasa przepięciowa: II 54. Parametry środowiskowe: RoHS 55. Temperatury otoczenia: 0°C do +45°C 56. Wilgotność otoczenia: 10 - 95% wilg. wzgl., brak kondensacji. |
|  | Inne | 1. Szafa musi być wyposażona w zintegrowany system wczesnego wykrywania i gaszenia pożaru panelem gaśniczymi o wysokości montażowej max. 1U. 2. Zastosowane urządzenie 1U powinno posiadać wew. zintegrowany pojemnik zawierający środek gaśniczy NOVEC1230 dla kubatury min. 2,8 m3. 3. Gaz przechowywany powinien być w zintegrowanych pojemnikach paneli jako ciecz, która paruje w dyszy gaśniczej i równomiernie rozprasza się w postaci gazu w strefie gaszenia ograniczonego do wnętrza zamkniętych szaf. 4. Środek gaśniczy nie powinien stanowić żadnego ryzyka dla ludzi przebywających w pomieszczeniu, do którego wyzwalany jest środek w stężeniu gaśniczym. 5. Środek gaśniczy wyzwalany powinien być do zamkniętych szaf jako bezbarwny, nieprzewodzący elektryczności i nie korozyjny gaz. Nie wymaga usuwania pozostałości po gaszeniu, nie pozostawia żadnych osadów. Pożar zostaje ugaszony przez odebranie energii cieplnej płomieniom. 6. Detekcja pożaru następowała będzie poprzez dwie czujki pożaru zintegrowane w panelu gaśniczym, powietrze z wnętrza szafy zasysane będzie i analizowane poprzez system dedykowanej instalacji. Informacje o alarmach, awariach, ostrzeżenia, wymaganej konserwacji przesyłane będą do systemu monitorowania warunków środowiskowych. 7. Panel gaśniczy musi posiadać niezależne zintegrowane zasilanie awaryjne na czas min. 4 godz. 8. Szafa 19” musi być wyposażona w czujniki otwarcia drzwi przednich i tylnych monitorujące ich otwarcie oraz rozbrojenie systemu gaszenia na czas otwarcia drzwi. |
|  | System monitorowania warunków środowiskowych | 1. Dla poprawnego działania dostarczonego systemu chłodzenia szafy IT oraz systemu gaszenia musi zostać zastosowany system zdalnego monitorowania warunków fizycznych. 2. System ten powinien być w pełni kompatybilny z funkcjonalnością dostarczonego urządzenia gaśniczego, chłodniczego oraz szafy IT. 3. System musi być oparty o centralną jednostkę sterującą posiadającą jeden adres IP, do której będzie można podłączyć min. 32 czujniki, elementy. 4. Jednostka centralna powinna być podłączona przez Ethernet do sieci danych, konfigurowana przez Web / USB, wysyłać alarmy przez serwer poczty elektronicznej oraz Moduł GSM. 5. Moduł GSM dla komunikacji SMS musi obsługiwać zakresy częstotliwości dla zakresu do 4G włącznie. 6. Dodatkowo powinna istnieć możliwość przesyłania powiadomień alarmowych z mini. 4 innych Modułów zarządzających spiętych w jedna sieć komunikacyjną. 7. Obsługiwane protokoły: TCP/IPv4, TCP/IPv6, SNMPv1, SNMPv2c, SNMPv3, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS, SMTP, Syslog, LDAP, Modbus TCP IP. 8. Zintegrowany WEB serwer 9. Zintegrowany serwer posiadający OPC UA, uniwersalny przemysłowy protokół komunikacyjny umożliwiający komunikację pomiędzy urządzeniami, odczytywanie danych z czujników przez system nadrzędnego sterowania 10. Port szeregowy komunikacyjny RS232 11. Możliwość obsługiwania funkcji Server Shutdown, automatycznego zamykania serwerów w zależności od występujących zdarzeń w ramach monitorowanych wybranych parametrów, wymaga określenia na etapie projektu ilości i typu sprzętu IP, klientów, określonych scenariuszy 12. Równoległa do SNMP możliwość komunikacyjna centralnego modułu monitorowania protokołem Modbus TCP IP 13. Stopień ochrony modułów monitoringu: min IP 30 wg PN-EN 60 529 14. Maks. łączna długość przewodów dla magistrali CAN-Bus w jednym module: 100m 15. Obsługa zasilania redundantnego dla modułu centralnego monitoring POE - Power over Ethernet 16. Zegar czasu rzeczywistego z NTP z buforem energii (24h) bez baterii/akumulatora 17. Zarządzanie użytkownikami: LDAP 18. Do zastosowanego systemu zdalnego monitoringu i zarządzania pracą urządzenia gaśniczego, urządzenia chłodniczego, dodatkowo musi zostać zastosowany w szafie 19” IT min. 1 czujnik dualny temperatura-wilgotności, czujnik wycieku punktowy oraz moduł wejścia – wyjścia dla sygnałów bez potencjałowych. 19. Czujnik dualny temperatura-wilgotność. Zakres pomiarowy temp.: 0°C…+55°C, dokładność pomiaru max. +- 1K, rozdzielczość pomiaru zmiany temp. max. 0.1 K. Zakres pomiarowy wilgotności względnej: 1… 99 %, dokładność pomiaru +- 3% w zakresie od 20 do 80% wilgotności względnej. Każdy z zastosowanych czujników temp./ wilgotności musi posiadać: możliwość ustawienia tzw. offsetu czyli korekcji zmierzonych wartości temp. i wilgotności, ustawienia progów wysokiego i niskiego stanu temp. i wilgotności osobno dla stanu ostrzeżenie i alarm, możliwość ustawienia histerezy w mierzonym zakresie temp. i wilgotności. 20. Moduł Wejścia-Wyjścia. Monitorowanie minimalnie ośmiu wejść cyfrowych i sterowanie za pomocą minimalnie czterech wyjść przekaźnikowych. W programie powinna istnieć możliwość połączenia przekaźników i wartości pomiarowych w taki sposób, aby załączały się w określonych okolicznościach. Oprogramowanie musi umożliwiać kontrolę urządzenia lub przekazywać komunikaty. Możliwość szybkiego podłączenia automatycznego rozpoznawania przez plug &play. 21. Zakres temperatury pracy: 0°C…+45°C |
|  | System automatycznego awaryjnego otwarcia drzwi szafy IT | 1. Szafa IT musi zostać wyposażona w zintegrowany system awaryjnego automatycznego otwarcia drzwi przednich i tylnych. 2. Automatyka systemu musi umożliwiać otwarcie drzwi szaf w sposób automatyczny w przypadku braku zasilania oraz awarii układu chłodzenia od ustawionego wzrostu temp. wewnątrz zamkniętej szafy. 3. Szaf musi być wyposażona w system otwarcia drzwi przednich i tylnych: lokalnego manualnego poprzez wkładkę zamka z przyciskiem, zdalnego po sieci oraz automatycznego w przypadku awarii i zadanej logicznej funkcji, scenariusza. W tym celu szafa powinna być wyposażona w odrębny niezależny moduł sterujący otwarciem drzwi szafy wraz z dedykowanym czujnikiem temp. NTC oraz lokalną informacją o granicznych i zadanych temp. wew. szafy. 4. Moduł sterujący zainstalowany w szafie powinien posiadać : 3 wejścia cyfrowe dedykowane dla sygnału alarmu z zewnętrznego systemu/ drzwi przednich / drzwi tylnych, 1 wejście dla czytników zamek cyfrowy / czytnik transponderów, 2 wyjścia dla systemu zwolnienia otwarcia drzwi, 2 wyjścia dla opcjonalnego elektrycznego systemu niwelowania podciśnienia w szafie, 2 złącza magistrali przyłączeniowej Can Bus. 5. System powinien być wyposażony w sterownik plug & play dla integracji z opcjonalnym oprogramowaniem DCIM Software. 6. System automatycznego awaryjnego otwarcia drzwi szafy powinien umożliwiać integrację oraz współpracę automatyki z zaprojektowanym wymiennikiem DX. 7. System musi umożliwiać zdalną konfigurację standardowo poprzez Web interfejs oraz opcjonalnie przez oprogramowanie DCIM. |
| **Licencja dostępowa** | | |
|  | Oprogramowanie | 1. MS Windows 2019 RDS CAL lub równoważne\* |
| **Oprogramowanie backupowe** | | |
|  | Tworzenie Kopii zapasowej | 1. Oprogramowanie backupowe obsługujące min. 1 fizyczny serwer bazodanowy oraz min. 2 hosty wirtualizacyjne ( zgodne z oprogramowaniem wirtualizacyjnym) wraz z 5 letnim okresem wsparcia 2. Obsługiwane systemy operacyjne Windows Serwer 2019, 2016,2012, Linux 3. Obsługiwane platformy minimum VMware i Hyper-V, a także do fizycznych serwerów i stacji roboczych oraz instancji chmurowych 4. Możliwość tworzenia spójnych aplikacyjnie kopii zapasowych maszyn wirtualnych na poziomie obrazu z zaawansowanym przetwarzaniem uwzględniającym specyfikę aplikacji (łącznie z obcinaniem dzienników transakcji). 5. Tworzenie przyrostowych kopii zapasowych poszczególnych maszyn wirtualnych w ramach istniejącego zadania backupu. 6. Udostępnianie macierzystej integracji z obiektową pamięcią masową, obejmującą środowisko lokalne, platformy AWS, Microsoft Azure i IBM Cloud oraz wiele rozwiązań pamięci masowej zgodnych z technologią S3. Pomaga zmniejszyć obciążenia finansowe związane z chmurą publiczną oraz wyeliminować przywiązanie do określonej marki urządzeń dodatkowej pamięci masowej. 7. Możliwość tworzenia dodatkowych migawek pamięci masowej w szerokiej gamie systemów pamięci podstawowej, takich jak HPE 3PAR StoreServ, HPE Nimble oraz NetApp ONTAP i HCI. 8. Pełna kopia syntetyczna 9. Wbudowane funkcje deduplikacji, kompresji i wykluczania plików wymiany 10. Powielanie kopii zapasowych 11. Kompleksowe szyfrowanie 12. Koligacja serwerów proxy 13. Integracja z deduplikującą pamięcią masową 14. Pliki kopii zapasowych poszczególnych maszyn wirtualnych 15. Przetwarzanie na poziomie obrazów z selekcją plików 16. Replikacja maszyn wirtualnych w oparciu o obrazy 17. Wspomagane przełączanie w tryb awaryjny i powrót po awarii 18. Replikacja z kopii zapasowej 19. Planowane przełączanie awaryjne 20. Przełączanie awaryjne jednym kliknięciem 21. Pełne odzyskiwanie maszyny wirtualnej 22. Odzyskiwanie dysków wirtualnych i plików maszyny wirtualnej 23. Portal odzyskiwania plików i maszyn wirtualnych dla operatorów działu wsparcia 24. Portal odzyskiwania elementów programu Microsoft Exchange dla operatorów działu wsparcia 25. Portal odzyskiwania baz danych Microsoft SQL 26. Portal odzyskiwania baz danych Oracle |
| **System typu NAC (Network Access Control)** | | |
| 1. | Wymagania minimalne | Przedmiotem zamówienia jest: Dostawa systemu kontroli dostępu do sieci wewnętrznej – system klasy NAC (Network Access Control) wraz z 36 miesięczną gwarancją producenta.   1. System kontroli dostępu musi być dostępny w postaci maszyny wirtualnej dostępnej na systemy wirtualizacyjne VMWare. System kontroli dostępu musi się składać z aplikacji zarządzającej pozwalającej na konfigurację systemu kontroli dostępu do sieci oraz serwerów RADIUS, które zapewniają uwierzytelnianie oraz autoryzację dostępu do sieci. Wymaga się, aby pojedynczy system kontroli dostępu był w stanie obsłużyć do co najmniej 300 systemów końcowych. 2. Zamawiający wymaga, aby dostarczony system był dostarczony z licencją umożliwiającą obsłużenie do co najmniej 300 systemów końcowych w systemie pracy HA na poziomie aplikacyjnym. 3. System kontroli dostępu musi zapewniać możliwość uwierzytelniania użytkowników (Proxy) do innych systemów uwierzytelniających RADIUS, LDAP/Microsoft Active Directory oraz lokalnej bazy użytkowników. Musi istnieć możliwość wyboru systemu uwierzytelniającego na podstawie:   Typu uwierzytelnienia np. IEEE 802.1x, MAC authentication (PAP, CHAP, MsCHAP, EAP- MD5), dostęp do zarządzania urządzeń itp.  Nazwy użytkownika, MAC adresu lub nazwy Host urządzenia.   1. Po przeprowadzeniu uwierzytelnienia musi następować autoryzacja dostępu do sieci. Wybór konkretnej autoryzacji dostępu musi być możliwy na podstawie następujących parametrów: 2. Typu uwierzytelniania np. IEEE 802.1x, MAC authentication, Management Authentication wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MsCHAP), MAC (MD5) itp. 3. Grupy użytkowników bazujące na grupach LDAP/Microsoft Active Directory, grupach RADIUS lub grupach nazw użytkowników wpisanych ręcznie 4. Systemów końcowych bazujących na nazwie systemu końcowego (Hostname), adresie IP, przynależności systemu końcowego do grupy LDAP/Microsoft Active Directory, MAC adresie 5. Typów urządzeń końcowych np. Android, iOS, Mac, Linux, Windows Mobile itp. 6. Lokalizacji – np. adresy IP przełączników, które przeprowadzają autoryzację wraz z możliwością wskazania konkretnych portów, SSID oraz konkretnych punktów dostępowych w przypadku sieci bezprzewodowej 7. Czasu – np. codziennie pomiędzy godziną 8:00 a 16:00. 8. Aplikacja powinna posiadać możliwość tworzenia profili autoryzacyjnych, które określają biznesową rolę użytkownika w sieci np.: Administrator, Księgowość, Radcy Prawni, Goście, Lekarze, Pracownicy itp. Rola taka powinna być powiązana z polityką jaką Zamawiający będzie chciał wymusić na urządzeniach klienckich (przełącznikach, sieci bezprzewodowej itp.). 9. Profil autoryzacyjny powinien wskazywać na politykę, jaka musi zostać wysłana do urządzenia aby zapewnić właściwą autoryzację dostępu systemu końcowego do sieci. 10. Polityka musi zapewniać możliwość wysłania standardowych atrybutów RADIUS w ramach których będzie możliwe ustawienie: sieci VLAN do której użytkownika ma mieć dostęp, listy kontroli dostępu ACL oraz Quality of Service. Ponieważ oprócz przydziału sieci VLAN różne urządzenia mogą wymagać wysłania różnych atrybutów istnieje konieczność zapewnienia możliwości definiowania wysyłanych atrybutów dla każdego urządzenia z osobna. Przykładowo dla większości przełączników przydzielenie systemu końcowego do sieci VLAN wymaga wysłania następujących atrybutów: Tunnel-Type, Tunnel-Medium-Type oraz Tunnel-Private-Group-ID. Ten ostatni atrybut zawiera faktycznie wymagany VLAN ID lub nazwę VLAN. Niektóre urządzenia posiadają własne atrybuty VSA (Vendor Specyfic Attributes). Polityka musi zapewniać możliwość wysyłania atrybutów VSA dla uzyskania odpowiedniej autoryzacji systemu końcowego w sieci. 11. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji CoA (Change of Authorization) zgodnie z RFC 3576 oraz RFC 5176. Ze względu na różną implementację powyższych RFC na różnych urządzeniach sieciowych wymaga się, aby istniała możliwość konfiguracji portu oraz formatu MAC adresu wysyłanego do urządzenia sieciowego w przypadku wymuszenia zmiany autoryzacji. 12. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji z wykorzystaniem protokołu SNMP – rozwiązanie stosowane przez niektórych producentów sprzętu sieciowego. 13. System kontroli dostępu musi zapewniać wsparcie dla wymuszenia zmiany autoryzacji poprzez wyłączenie i włączenie portu. 14. System kontroli dostępu musi zapewnić interfejs konfiguracyjny pracujący w architekturze klient/serwer. Preferowane jest rozwiązanie korzystające z przeglądarki www. 15. System kontroli dostępu musi zapewniać bieżącą widzialność dopuszczonych do sieci systemów końcowych. Wymaga się, aby widziane były następujące parametry systemu końcowego i jego stanu: 16. MAC adres systemu końcowego 17. Adres IP systemu końcowego 18. Nazwa komputera – Host Name 19. Typ systemu końcowego oraz system operacyjny – możliwość wykrywania urządzeń na podstawie zapytań DHCP (DHCP fingerprinting) np. Windows/ Windows 2012, iPhone/Android itp. 20. Nazwa urządzenia, do którego dołączony jest klient – to może być nazwa kontrolera bezprzewodowego lub nazwa przełącznika sieciowego. 21. Adres IP urządzenia, do którego dołączony jest klient i które przeprowadza uwierzytelnienie i autoryzację systemu końcowego 22. Typ uwierzytelniania systemu końcowego np. MAC authentication, IEEE 802.1x wraz z informacją o wykorzystywanym protokole EAP np. PEAP, EAP-MD5, EAP-TLS itp. 23. System kontroli dostępu musi zapewniać przechowywanie historii dostępu systemu końcowego do sieci. 24. System kontroli dostępu musi zapewniać możliwość wymuszenia ponownej autoryzacji wskazanego systemu końcowego z wykorzystaniem wymaganych powyżej funkcjonalności CoA. 25. System kontroli dostępu musi zapewniać możliwość szybkiego przeniesienia wskazanego systemu do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci tzw. grupa Black List. 26. System kontroli dostępu musi umożliwiać uruchomienie systemu kontroli dostępu do sieci poprzez stronę www tzw. Captive Portal. 27. System kontroli dostępu musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa. 28. Agent musi być dostępny min. na systemy operacyjne Windows oraz MAC OS. 29. System musi zapewniać współpracę z systemami MDM (Mobile Device Management) w celu sprawdzania zgodności z polityką bezpieczeństwa dla urządzeń mobilnych. 30. System kontroli dostępu powinien posiadać interfejs API pozwalający na prostą integrację systemu kontroli dostępu z systemami 3rd party. |
| 2. | Gwarancja | 1. Przedmiot zamówienia objęty będzie 36 miesięczną gwarancją świadczoną w miejscu użytkowania Systemu. 2. Bieg terminu gwarancji rozpoczyna się z chwilą podpisania bez zastrzeżeń Protokołu Uruchomienia Usług przez obie Strony. Wszelkie koszty napraw gwarancyjnych, w tym koszty transportu ponosi Wykonawca. 3. W trakcie 36 miesięcy w ramach gwarancji, Zamawiający będzie uprawniony do pobierania nowych wersji oprogramowania, które zostanie zaoferowane w ramach Zamówienia. 4. Usługa gwarancji zapewni minimum: 5. Udzielanie odpowiedzi na pytania dotyczące instalacji, używania i konfiguracji Systemu używanego przez Zamawiającego. 6. Bezpośrednie konsultacje telefoniczne oraz poprzez pocztę elektroniczną z inżynierem producenta dotyczące bieżących problemów związanych z Systemem (w dni robocze w godzinach 7:00 - 16:00). 7. Analizę informacji diagnostycznych mająca na celu określenie przyczyny problemu, np. pomoc w interpretacji dokumentacji problemów związanych z instalacją lub kodem. 8. W przypadku znanych defektów oprogramowania, przekazywanie informacji o sposobie ich usunięcia lub obejścia, a także udzielanie pomocy w uzyskaniu poprawek, do otrzymania których Zamawiający jest uprawniony w ramach posiadanej licencji. 9. Czas na potwierdzenie przyjęcia zlecenia i rozpoczęcia konsultacji nie dłuższy niż 4 godziny robocze. 10. Maksymalny czas odpowiedzi na zgłoszoną konsultację 4 dni robocze. 11. Obsługę zgłoszeń w języku polskim 12. W ramach gwarancji Wykonawca zapewni co najmniej: 13. Możliwość telefonicznego oraz elektronicznego zgłaszania awarii dotyczących sprzętu w dni robocze, w godzinach 8:00-16:00 w trakcie trwania okresu gwarancji. 14. Do awarii zgłoszonej po godz. 15.00 dnia poprzedzającego dzień ustawowo wolny od pracy i sobotę wykonawca przystąpi o godz. 8.00 pierwszego dnia roboczego.Za awarie uznaje się błąd uniemożliwiający eksploatacje urządzenia Systemu i nie pozwalający na znalezienie przez Zamawiającego takiego sposobu używania, aby skutecznie obejść jego przyczyny. Za czas reakcji uznaje się czas od momentu zgłoszenia awarii bądź usterki przez Zamawiającego do momentu podjęcia przez Wykonawcę czynności zmierzających do usunięcia awarii lub usterki. Czas reakcji nie dłuższy niż 8 godzin. 15. Nieprzerwany i nieograniczony dostęp do zasobów elektronicznych, baz samopomocy, FAQ (ang. Frequently Asked Questions), baz wiedzy producenta oprogramowania. 16. Usunięcie awarii w terminie do 24 godzin od momentu zgłoszenia, z zastrzeżeniem że termin usunięcia awarii zgłoszonej po godz. 15.00 w dniu poprzedzającym dzień ustawowo wolny od pracy i sobotę liczony będzie od godziny 8.00 pierwszego dna roboczego. W sytuacjach szczególnych, jeżeli Wykonawca mimo nieprzerwanego prowadzenia prac nad usunięciem awarii lub usterki, nie będzie w stanie z przyczyn od siebie niezależnych, usunąć awarii lub usterki w terminie określonym powyżej, Zamawiający na wniosek Wykonawcy może przedłużyć ten termin bez naliczania kar umownych. 17. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, pobieranie uaktualnień oraz poprawek oprogramowania. |

Dla elementów, dla których nie zostały określone warunki gwarancji, obowiązują **Podstawowe warunki gwarancji określone w punkcie 3.3. OPZ.**

\* **Warunki równoważności na dostarczane oprogramowanie**

Zamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia, jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności  
i będzie kompatybilne w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego.

Za rozwiązanie równoważne Zamawiający uznaje rozwiązanie, które nie spowoduje poniesienia dodatkowych kosztów (np. dodatkowych licencji, dodatkowego sprzętu, kosztów związanych  
z modyfikacją systemów działających u Zamawiającego, itp.) po stronie Zamawiającego.