**Załącznik nr 1 do OPZ**

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

**Specyfikacja przedmiotu zamówienia w obszarze infrastruktury teleinformatycznej**

**dla**

**Uniwersyteckiego Szpitala Ortopedyczno-Rehabilitacyjnego w Zakopanem**

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.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Typ** | **Liczba zamawianego sprzętu (sztuk)** |
|  | Serwer (2 CPU 12 rdzeni) | 2 |
|  | Zewnętrzny napęd taśmowy | 1 |
|  | Zewnętrzna pamięć masowa | 1 |
|  | Sprzęt komputerowy – zestaw stacjonarny | 25 |
|  | Sprzęt komputerowy - laptopy | 3 |
|  | Przełączniki szkieletowe | 2 |
|  | Akcesoria przełączników szkieletowych | 26 |
|  | Szafa Rack 47U | 1 |
|  | System klasy DLP | 1 |
|  | System klasy NAC | 1 |
|  | Urządzenia wielofunkcyjne | 6 |

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** |
| --- | --- | --- |
| **Serwer (2 CPU 12 rdzeni)** | | |
| 1. | Obudowa | Obudowa typu Rack o wysokości maksymalnej 2U (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)  Serwer wyposażony w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. |
| 2. | Procesor | Dwa procesory dwunastodzeniowe o częstotliwości min 3,2GHz , x86 - 64 bity, Procesor musi być wykonany w technologii x86-64. Procesor musi osiągać przynajmniej 33741 punkty wydajności według <https://www.cpubenchmark.net/> na dzień 13-01-2020  Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz |
| 3. | Pamięć RAM | 256 GB w modułach o pojemności 32GB każdy. |
| 4. |  | Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Wsparcie dla technologii zabezpieczania pamięci Advanced ECC/SDDC, Rank sparing (online spare), Demand i Patrol scrubbing, Memory thermal control, Failed DIMM isolation lub równoważnych.  Serwer z obsługą pamięci typu NVDIMM |
| 5. | Sloty PCI Express | 3 aktywne gniazda PCI-Express generacji 3, w tym min. 2 slot x16 (szybkość slotu – bus width)  2 gniazda PCI-Express generacji 3 |
| 6. | Wbudowane porty | Porty graficzne wyprowadzone na froncie i tyle obudowy;  Min. 5 portów USB 3.0 w tym 1szt. na froncie obudowy 2 szt. wewnątrz obudowy;  Min. port szeregowy, wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45;  Ilość dostępnych złączy graficznych i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy itp.  Wewnętrzny slot na kartę micro SD lub SD |
| 7. | Karta graficzna | Zintegrowana karta graficzna |
| 8. | Interfejsy | Minimum 4 zintegrowane z płytą główną porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE.  Minimum dodatkowe 2 porty 10Gb Base-T. |
| 9. | Wewnętrzna pamięć masowa | Zainstalowane 2 dyski SSD o pojemności 480GB SSD SATA do zastosowań mieszanych (Mixed Use).  Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy  W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD 2,5”typu Hot Swap. |
| 10. | Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.  Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania.  Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie |
| 11. | Zasilacze | 2 szt., typu Hot-plug, redundantne, każdy o mocy max. 500W. |
| 12. | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug.  Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia równej 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A3 |
| 13. | Napęd | Wbudowany wewnętrzny napęd DVD-ROM lub DVD-RW |
| 14. | Karta/moduł zarządzający | Niezależna od system 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: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe  wparcie dla agentów zarządzających oraz możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP  dostęp do karty zarządzającej poprzez  dedykowany port RJ45 z tyłu serwera  przez współdzielony port zintegrowanej karty sieciowej serwera  dostęp do karty możliwy  z poziomu przeglądarki webowej (GUI)  z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)  z poziomu skryptu (XML/Perl)  poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)  wbudowane narzędzia diagnostyczne  zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego  obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie  wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników  przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)  obsługa zdalnego serwera logowania (remote syslog)  wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów  mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie  funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności  monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji  konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)  zdalna aktualizacja oprogramowania (firmware)  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  możliwość równoczesnej obsługi przez 6 administratorów  autentykacja dwuskładnikowa (Kerberos)  wsparcie dla Microsoft Active Directory  obsługa SSL i SSH  enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli  wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API  wsparcie dla Integrated Remote Console for Windows clients  możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |
| 15. | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2012 R2, 2016, 2019  Red Hat Enterprise Linux (RHEL) 7, 8  SUSE Linux Enterprise Server (SLES) 11, 12, 15  CentOS 7.4  VMware ESXi 6.5, 6.7, 6.7U3 |
| 16. | Gwarancja | Serwer objęty jest minimum 3 letnią gwarancją producenta w miejscu instalacji z czasem reakcji serwisu najpóźniej na następny dzień roboczy od dnia zgłoszenia.  Serwis gwarancyjny świadczony jest przez serwis producenta oferowanego serwera.  Wszystkie wymagane licencje muszą być składnikiem serwera oraz mają być przypisane do sprzętu na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań.  Możliwość sprawdzenia statusu gwarancji i pełnej konfiguracji oferowanego serwera na stronie producenta po podaniu nr seryjnego serwera.  Serwer w pełnej oferowanej konfiguracji musi być przypisany do Zamawiającego w systemie producenta serwera.  Urządzenia na etapie dostawy Producent a Zamawiający nie mogą podlegać modyfikacjom w zakresie konfiguracji sprzętowej.  Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.).  Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne.  W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania. |
| 17. | Inne | Wszystkie użyte do budowy elementy musza znajdować się w ogólnodostępnych kartach katalogowych producenta serwera.  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.  Serwer musi posiadać deklaracje CE lub równoważną – załączyć do oferty.  Przez dokument równoważny zamawiający rozumie taki, który potwierdza zgodność oferowanych urządzeń co najmniej z:  ­ R & TTE 1999/5/EC1,  ­ rozporządzeniem Komisji (WE) nr 1275/2008,  ­ przepisami dyrektywy ErP 2009/125/WE.  Serwer musi być wyprodukowany zgodnie z normą ISO-9001 lub równoważną - załączyć do oferty dokument poświadczający. Przez normę równoważną zamawiający rozumie taką, która co najmniej:  ­ określa politykę jakości organizacji;  ­ określa wymagania dotyczące wyrobu oraz umożliwia ich przegląd;  ­ określa cele w zakresie jakości wyrobów;  ­ reguluje kwestie odpowiedzialności kierownictwa;  ­ definiuje uprawnienia pracowników;  ­ definiuje politykę środowiskowa organizacji;  ­ określa jej cele, zadania i programy środowiskowe;  ­ definiuje i wskazuje niezbędne zasoby, role, odpowiedzialność  i uprawnienia;  ­ opisuje sterowanie operacyjne oraz gotowość i czasy reakcji na awarie;  ­ wskazuje metody monitorowania i pomiaru wyrobów i procesów.  W ramach dostawy, Wykonawca zainstaluje sprzęt w szafach serwerowych Zamawiającego oraz dokona podstawowej konfiguracji sprzętu oraz oprogramowania systemowego w uzgodnieniu z Zamawiającym. Wykonawca winien uwzględnić minimum 3 dni robocze pracy inżyniera dla wykonania prac instalacyjnych i konfiguracyjnych. |
| **Zewnętrzny napęd taśmowy** | | |
| 1. | Obudowa | Możliwość instalacji w szafie Rack 19”, wysokość nie więcej niż 2U. |
| 2. | Obsługiwane napędy | LTO Ultrium 5,  LTO Ultrium 6,  LTO Ultrium 7,  LTO Ultrium 8. |
| 3. | Interfejsy napędów | Możliwość montażu napędów z interfejsami 6Gb SAS lub 8Gbps FC typu Hot-Swap. |
| 4. | Liczba napędów | Obsługa do 2 napędów HH. Biblioteka w chwili dostawy powinna być wyposażona w 1 napędy LTO Ultrium 8, połówkowej wysokości z interfejsem SAS, wraz z niezbędnym okablowaniem o długości min. 3 mb. Dodatkowo Wykonawca dostarczy i zainstaluje kartę HBA SAS 12Gb na złączu PCI-E, kompatybilną z posiadanym przez Zamawiającego serwerem HPE PROLIANT DL380G10 LFF |
| 5. | Liczba slotów | Biblioteka powinna umożliwiać obsługę do minimum 24 taśm magnetycznych. |
| 6. | Obsługiwane nośniki | LTO8: 12TB natywnie,  LTO7: 6TB natywnie,  LTO6: 2,5TB natywnie,  LTO5: 1,5TB natywnie.  Wsparcie dla taśm typu WORM.  Biblioteka powinna być wyposażona w minimum 2 taśmy czyszczące oraz minimum 24 taśmy LTO7 zgodne z formatem M7. |
| 7. | Oprogramowanie | Biblioteka musi być wyposażona w oprogramowanie, które może przewidywać awarie i zapobiegać im poprzez wczesne ostrzeganie, a także sugerować wymagane działania serwisowe.  Oferowane oprogramowanie ma mieć możliwość określenia, kiedy wycofać kasety z taśmą i jaki stopień kompresji jest osiągany. |
| 8. | Zarządzanie | Wyposażona w panel operatorski z diodami sygnałowymi i wyświetlaczem.  Dostępny minimum 1 port minimum 10/100/1000Mb dla zarządzania zdalnego poprzez interfejs WWW. |
| 9. | Inne | 1 kabel SAS kompatybilny z dostarczaną biblioteką oraz kartą HBA o długości min. 3 mb  Odpowiednie licencje producenta, jeśli są przewidywane, do pełnej obsługi dla 1 napędu, 24 taśmy. |
| 10. | Gwarancja | minimum 3 letni okres gwarancji producenta w miejscu instalacji.  W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania |
| **Zewnętrzna pamięć masowa** | | |
|  | Definicja | Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych kontrolowanych przez dedykowane kontrolery macierzowe [bez dodatkowych urządzeń pośrednich, serwerów wirtualizujących itp.]. |
|  | Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19” lub dostarczana w specjalnie dostosowanej dla niej szafie rack. |
|  | Przestrzeń dyskowa | Macierz musi udostępniać minimum 36,7 TB przestrzeni użytkowej dla danych, w tym minimum:   * Min. 4,1 Tb przestrzeni użytkowej zbudowanej w oparciu o dyski w technologii SSD, zabezpieczonych mechanizmem RAID5. * Min**.** 32,6 TB przestrzeni użytkowej zbudowanej w oparciu o dyski w technologii SAS i prędkości obrotowej min. 10k obr/min, zabezpieczonych mechanizmem RAID6.   Wszystkie dyski danej klasy muszą mieć identyczne parametry pojemnościowe i wydajnościowe. |
|  | Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę bez wymiany kontrolerów macierzy, do co najmniej 240 dysków twardych, w tym do 120 dysków SSD.  Dla zapewnienia najwyższej wydajności, maksymalna konfiguracja macierzy musi wspierać tworzenie wolumenów rozłożonych na wszystkich dyskach macierzy (tzw. wide-striping) i ich jednoczesne, aktywne udostępnianie ze wszystkich kontrolerów macierzy. |
|  | Obsługa dysków | Macierz musi obsługiwać dyski SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i Nearline SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
|  | Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1 lub 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).  Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, kontroler, zasilacz.  Możliwość definiowania różnych poziomów RAID na tych samych dyskach fizycznych. Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, dla uzyskania podobnej wydajności wymagane jest zrealizowanie żądanej pojemności większą o 50% liczbą dysków fizycznych.  Macierz musi umożliwiać definiowanie globalnych dysków spare lub odpowiedniej zapasowej przestrzeni dyskowej. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare lub odpowiednią zapasową przestrzeń dyskową. |
|  | Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC.  Komunikacja pomiędzy wszystkimi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem protokołów FC/Ethernet/Infiniband).  Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt/zapis) wszystkich wolumenów utworzonych w ramach całego systemu dyskowego. Macierz wyposażona w połączenia dyskowe min. SAS 12 Gb. |
|  | Pamięć cache | Każdy kontroler macierzowy musi być wyposażony w minimum 32 GB pamięci cache, 64 GB sumarycznie w macierzy dla dwóch kontrolerów. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć cache musi mieć możliwość dynamicznego przydziału zasobów dla zapisu lub odczytu.  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 | * Macierz musi umożliwiać rozbudowę przestrzeni cache za pomocą dysków SSD do minimum 832 GB. Taka przestrzeń, musi być dostępna zarówno dla zasobów blokowych jak i plikowych. Jeżeli taka funkcjonalność nie jest dostępna, należy zaoferować rozwiązanie wyposażone, w co najmniej 128 GB DRAM cache. |
|  | Interfejsy | Macierz musi posiadać, co najmniej:  - min. 2 porty Ethernet 1 Gb/s (oba porty Ethernet przeznaczone do zdalnej replikacji danych).  - min. 4 porty iSCSI 10 Gb/s   * - min. 4 porty 10 Gb/s Eth przeznaczone dla protokołów plikowych CIFS i NFS). |
|  | Zarządzanie | Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego.  Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wewnętrznych, grup dyskowych, dysków logicznych (LUN), pojedynczych napędów dyskowych oraz kontrolerów. Konieczne jest analizowanie wymienionych parametrów na bazie danych historycznych.   * Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
|  | Zarządzanie grupami dyskowymi oraz dyskami logicznymi | * Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności woluminów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych. Musi być możliwość zdefiniowania, co najmniej 8000 woluminów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego dysku/woluminu logicznego na wszystkie dyski fizyczne macierzy(tzw. wide striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli funkcjonalność tzw. wide-striping w oferowanej macierzy nie jest dostępna to należy wyposażyć macierz w 50% więcej przestrzeni dyskowej brutto dla każdego typu dysków wymienionych w punkcie Wymagana przestrzeń dyskowa z ew. niezbędnymi licencjami. |
|  | 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 dostarczanego 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 konieczności wcześniejszego 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 wspierać minimum 2048 kopii migawkowych per wolumen logiczny i minimum 65000 wszystkich kopii migawkowych. |
|  | Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID. Musi być możliwość wykonania kopii w innej grupie dyskowej niż dane oryginalne.   * Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
|  | Dostęp plikowy | Macierz musi wspierać natywnie dostęp plikowy za pomocą tych samych kontrolerów, które obsługują dostęp blokowy.   * Oferowane rozwiązanie musi wspierać integrację z oprogramowaniem antywirusowym. |
|  | 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. 3 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 dostarczanego urządzenia. |
|  | Zdalna replikacja danych | Macierz musi umożliwiać zdalną replikację danych typu online 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. Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych infrastruktur (FC, sieci IP).   * Wymagana jest dostarczenie opisanej funkcjonalności. |
|  | Ciągła dostępność do danych | Macierz musi umożliwiać uruchomienie replikacji synchronicznej z inną macierzą z tej samej rodziny i zapewniać – w przypadku awarii i całkowitej niedostępności jednej z macierzy – bezprzerwową pracę systemów działających na platformie przetwarzania danych i korzystających z zasobów pamięci masowych. Opisana powyżej obsługa awarii (przełączenie między macierzami) musi odbywać się w sposób automatyczny i transparenty (bez przerywania dostępu do danych) dla korzystających z macierzy hostów. Opisana funkcjonalność musi integrować się z platformą wirtualizacyjną VMware ESX i posiadać certyfikację VMware vSphere Metro Storage Cluster, potwierdzoną wpisem na ogólnodostępnej liście kompatybilności producenta. Nie dopuszcza się rozwiązania, które wymaga dodatkowych urządzeń do obsługi powyższej funkcjonalności.   * Wymagana jest możliwość aktywowania opisanej funkcjonalności w przyszłości poprzez ew. dokupienie odpowiednich licencji w przyszłości. |
|  | Zarządzanie wydajnością | Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS (możliwość definiowania progów minimalnych i maksymalnych) dla wybranych wolumenów logicznych.   * Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
|  | Deduplikacja i kompresja danych | Macierz musi umożliwiać deduplikację i kompresję danych na poziomie blokowym. Musi istnieć możliwość uruchomienia deduplikacji i kompresji na poziomie pojedynczych wolumenów logicznych. Deduplikacja i kompresja danych musi odbywać się w locie, przed zapisaniem danych na dyskach macierzy. Musi istnieć możliwość wykonania operacji odwrotnej – wyłączenia deduplikacji i kompresji na określonych wolumenach logicznych.  Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, wymagane jest dostarczenie większej o 50% pojemności użytkowej macierzy (co najmniej w odniesieniu do dysków SSD).   * Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
|  | Redundancja | 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 dwóch niezależnych źródeł zasilania –odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy.   * Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii. |
|  | Dostęp plikowy | Macierz musi umożliwiać udostępnianie danych plikowych po protokołach CIFS (min. SMB v3) i NFS (min. NFS v4) bezpośrednio ze wszystkich kontrolerów macierzowych obsługujących ruch blokowy.   * Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
|  | 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.   * Instalacja lub uruchamianie dodatkowej funkcjonalności macierzy dyskowej nie może powodować zmniejszenia dostępnego obszaru pamięci cache danych kontrolerów macierzowych. W ramach dostawy należy również dostarczyć dwa przełączniki SAN wyposażone w minimum 8 portów aktywnych 16gb każdy oraz zestaw okablowania |
|  | Gwarancja | Macierz objęta minimum 3 letnim okresem gwarancji producenta w miejscu instalacji z czasem reakcji serwisu najpóźniej na następny dzień roboczy od dnia zgłoszenia.  Serwis gwarancyjny realizowane jest przez serwis producenta oferowanej macierzy.  Uszkodzony dysk po wymianie pozostaje u użytkownika (ochrona dysków).  Usługa napraw gwarancyjnych musi być świadczona przez autoryzowany przez producenta serwis. Czas diagnozy problemu nie wydłuża czasu naprawy, jest w niego już wliczony.  Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.).   * Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne.   W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania |
|  | 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 normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE.   * Urządzenia fabrycznie nowe, nieużywane, nie rekondycjonowane, nie powystawowe, rok produkcji - 2018 |
| **~~Backup oprogramowanie~~** | | |
| 1. | ~~Wymagania ogólne~~ | ~~W ramach środowiska należy dostarczyć licencję oprogramowania w wersji obsługującej do minimum 6 procesorów fizycznych zainstalowanych w serwerach wraz gwarancją na okres 3 lat od dostawy do Zamawiającego~~  ~~• Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0, 6.5 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej~~  ~~• Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.~~  ~~• Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.~~  ~~• Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V~~  ~~• Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone~~  ~~• Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej~~  ~~• Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków~~  ~~• Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji~~  ~~• Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.~~  ~~• Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.~~  ~~• Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania~~  ~~• Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia~~  ~~• Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie~~  ~~• Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.~~  ~~• Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)~~  ~~• Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10, 8.20, 9.0 i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.~~  ~~• Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji~~  ~~• Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji~~  ~~• Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza~~  ~~• Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)~~  ~~• Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.~~  ~~• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej~~  ~~• Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych~~  ~~• Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora~~  ~~• Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn~~  ~~• Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server~~  ~~• Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej~~  ~~• Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)~~  ~~• Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.~~  ~~• Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.~~  ~~• Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.~~  ~~• Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.~~  ~~• Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik~~  ~~• Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)~~  ~~• Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V~~  ~~• Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)~~  ~~• Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere~~  ~~• Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)~~  ~~• Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania~~  ~~• Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami~~  ~~• Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków~~  ~~• Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure.~~  ~~• Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików~~  ~~• Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.~~  ~~• Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:~~  ~~− Linux ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs~~  ~~− BSD UFS, UFS2~~  ~~− Solaris ZFS, UFS~~  ~~− Mac HFS, HFS+~~  ~~− Windows NTFS, FAT, FAT32, ReFS~~  ~~− Novell OES NSS~~  ~~• Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.~~  ~~• Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.~~  ~~• Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.~~  ~~• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),~~  ~~• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat~~  ~~• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.~~  ~~• Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.~~  ~~• Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.~~  ~~• Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.~~  ~~• Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows~~  ~~• Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN~~  ~~• Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.~~  ~~• Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem~~  ~~• Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere~~  ~~• System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich~~  ~~• System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x, 6.0 oraz 6.5 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie~~  ~~• System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.~~  ~~• System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware~~  ~~• System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter~~  ~~• System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn~~  ~~• System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel~~  ~~• System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk~~  ~~• System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora~~  ~~• System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów~~  ~~• System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)~~  ~~• System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna~~  ~~• System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego~~  ~~• System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta~~  ~~• System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.~~  ~~• System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware~~  ~~• System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 5.5, 5.6, 8.0 oraz 8.10~~  ~~• System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 4.1, 5.x, 6.0 oraz 6.5, vCenter Server 4.1, 5.x, 6.0 oraz 6.5 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2i 2016.~~  ~~• System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.~~  ~~• System musi być certyfikowany przez VMware i posiadać status „VMware Ready”~~  ~~• System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V~~  ~~• System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF~~  ~~• System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc~~  ~~• System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach~~  ~~• System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów~~  ~~• System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych~~  ~~• System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych~~  ~~• System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury~~  ~~• System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta~~  ~~• System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.~~  ~~• System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.~~  ~~• System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware~~  ~~• System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)~~  ~~System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie~~ |
| 2. |  | ~~3 lata gwarancji~~  ~~W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania~~  ~~Wykonawca zrealizuje instalację I konfigurację oferowanego rozwiązania w środowisku Zamawiającego po uprzednim przedstawieniu projektu wdrożenia Zamawiającemu. Zamawiający wymaga aby Wykonawca zapewnił łącznie 2 dni robocze pracy inżyniera systemowego w ramach wdrożenia system backup. Na etapie zawarcia umowy Zamawiający przekaże informacje techniczne niezbędne Wykonawcy do przygotowania projektu wdrożenia~~ |
| **Sprzęt komputerowy – zestaw stacjonarny** | | |
|  | | Komputer PC |
| 1. | Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| 2. | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| 3. | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 8000 punktów, załączyć do oferty wyniki przeprowadzonego testu |
| 4. | Pamięć operacyjna RAM | 8GB DDR4 2400MHz non-ECC możliwość rozbudowy o min 32GB, minimum 2 gniazda wolne |
| 5. | Parametry pamięci masowej | 256 GB SSD |
| 6. | Wyposażenie multimedialne | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. audio out. |
| 7. | Obudowa | Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w min. 2 kieszenie 2,5” wewnętrzne, Napęd optyczny  w dedykowanej wnęce zewnętrznej slim. Obudowa powinna fabrycznie umożliwiać montaż min 2 szt. dysku. Obudowa fabrycznie przystosowana do pracy w orientacji pionowej. Wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. Wymaga się min. 2 otwory wentylacyjne zapewniające cyrkulację powietrza przód -> tył.  Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus,  w przypadku kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.  Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 2,5” bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa w jednostce centralnej musi być zabezpieczona śrubami radełkowymi. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisk POWER [ tzn. barw i miganie ] W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej [ w tym również portów I/O, chipset ], awarię CMOS baterii, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych  w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| 8. | Zgodność z systemami operacyjnymi | Oferowane modele komputerów muszą poprawnie współpracować  z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). |
| 9. | Bezpieczeństwo | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia  i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności: testy uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów. podsumowanie testów z możliwością zapisywania wyników, uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu. Uruchamianie testów zdefiniowanych przez użytkownika, wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów, wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów. Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera. Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, typ pamięci wraz z taktowanie oraz SN i PN, wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz. System działający nawet w przypadku braku dysku twardego lub w przypadku jego uszkodzenia, pozwalający na uzyskanie wyżej wymienionych funkcjonalności a w szczególności na przetestowanie: procesora i pamięci. W przypadku braku możliwości uruchomienia graficznego systemu diagnostycznego komputer musi zawierać w sobie dodatkowo niezależny system diagnostyczny wizualny oparty o sygnalizację świetlną informujący użytkownika o awarii (system opisany przy obudowie). |
| 10. | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| 11. | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera,  Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego ) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie produkcji komputera, włączonej lub wyłączonej funkcji aktualizacji BIOS, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, aktywnym kanale – dual channel, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, maksymalnej osiąganej prędkości zainstalowanego procesora, pamięci cache L2 zainstalowanego procesora, pamięci cache L3 zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dyskach twardych podpiętych do dostępnych na płycie głównej portów SATA oraz M.2, rodzajach napędów optycznych, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej  z zewnętrznych urządzeń.  Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.  Możliwość włączenia/wyłączenia kontrolera SATA ( w tym w szczególności pojedynczo)  Możliwość włączenia/wyłączenia kontrolera audio,  Możliwość włączenia/wyłączenia układu TPM.  Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB,  Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLAN– opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN,  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  Funkcja zbierania i zapisywania incydentów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę oraz opis incydentu kodu wizualnego systemu diagnostycznego.  Funkcja pozwalająca na włączenie/wyłączenie automatycznego tworzenia recovery BIOS na dysku twardym lub na urządzeniu zewnętrznym podpiętym przez USB  Możliwość wyłączania portów USB pojedynczo  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min.: uruchamianie systemu  z serwera za pośrednictwem zintegrowanej karty sieciowej, wejścia do BIOS, upgrade BIOS bez konieczności uruchamiania systemu operacyjnego oraz dostępu do sieci LAN lub internetu, |
| 12. | Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001  Deklaracja zgodności CE (załączyć do oferty)  Certyfikat TCO, wymagana certyfikacja na stronie: <http://tco.brightly.se/pls/nvp/!tco_search> – załączyć do oferty wydruk  z strony  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności  z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram |
| 13. | 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 22 dB (załączyć oświadczenie producenta) |
| 14. | Warunki gwarancji | Firma świadcząca usługi serwis gwarancyjnego musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia producenta potwierdzając, że serwis gwarancyjny urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta.  Minimalny czas gwarancji producenta wynosi 3 lat od daty dostawy.  Sposób realizacji usług gwarancji:   * Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. * Dedykowany bezpłatny portal online do zgłaszania usterek   i zarządzania zgłoszeniami serwisowymi.   * Możliwość kontaktu za pośrednictwem mediów społecznościowych (czat online, Facebook, Twitter) w sprawie usterek i problemów zidentyfikowanych podczas eksploatacji   Serwis gwarancyjny dla sprzętu będzie świadczony zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta.  Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii do serwisu gwarancyjnego.  Zamawiający wymaga od podmiotu realizującego serwis gwarancyjny lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| 16. | System operacyjny | Zainstalowany system operacyjny Windows 10 Professional lub równoważny\*, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| 16. | Wymagania dodatkowe | Wbudowane porty:  1x DisplayPort v1.1a  1x HDMI 1.4  1x VGA  1x LAN 10/100/1000 wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Porty USB  Panel przedni  - 4x USB w układzie 2x USB 3.1 TYP A i 2x USB 2.0  Panel Tylny  - 4x USB w układzie 2x USB 3.1 TYP A i 2x USB 2.0  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB TYP-A nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane  z obudową (wlutowane w laminat płyty głównej).  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w:  1 złącza PCI Express x16 Gen.3,  3 złącza PCI Epress x1,  2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM,  3 złącza SATA w tym 2 szt SATA 3.0;  1 złącze M.2 2280 dedykowane dla syków M.2 SATA lub NVMe  1 złącze M.2 WLAN  1 konektor realizujący funkcję clear CMOS  1 konektor realizujący funkcję clear Password  Klawiatura USB w układzie polski programisty  Mysz USB z rolką (scroll)  Nagrywarka DVD +/-RW o prędkości min. 8x  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. |
| 17. | Oprogramowanie biurowe | Równoważność dla MS Office Dla użytkowników domowych i małych firm.  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:  a) Edytor tekstów  b) Arkusz kalkulacyjny  c) Narzędzie do przygotowywania i prowadzenia prezentacji  d) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)  8. 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) Wydruk dokumentów  k) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną  l) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 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 2010, 2013 i 2016.  m) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  9. 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 np.: inne arkusze kalkulacyjne  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 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 2010, 2013 i 2016.  m) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a) 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 2010, 2013 i 2016. Zapewnienie po edycji i zapisaniu danego dokumentu bezproblemową jego dalszą pracę w programach Microsoft PowerPoint 2010, 2013 i 2016.  11. 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    W szczególności Wykonawca musi zapewnić stabilność i pełną wymaganą funkcjonalność współpracy z posiadanym przez Zamawiającego następującym oprogramowaniem:  - pełną zgodność z formatami plików utworzonych za pomocą oprogramowania MS Office |
|  | | Monitor do komputera PC |
| 1. | Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą min. 24” (16:9) |
| 2. | Rozmiar plamki | Maks. 0,28 mm |
| 3. | Jasność | Min. 250 cd/m2 |
| 4. | Kontrast | Typowy min. 1000:1 |
| 5. | Rozdzielczość maksymalna | Min. 1920 x 1080 |
| 6. | Podświetlenie | System podświetlenia LED |
| 7. | Zabezpieczenia | Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.  Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie (kwestia karty graficznej czy monitora) |
| 8. | Pochylenie | Wymagany, od -5 do +22 stopni |
| 9. | Kolor | Czarny |
| 10. | Złącza | 1x 15-stykowe złącze D-Sub,  1x DisplayPort  1 x HDMI |
| 11. | Gwarancja | 3 lat na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego |
| 12. | certyfikaty | TCO, ISO 13406-2 lub ISO 9241, Energy Star |
| **Sprzęt komputerowy - laptopy** | | |
| 1. | Procesor | 1) Procesor klasy x86 ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych, zapewniający wydajność całego oferowanego laptopa (Rating) min. 1450 pkt w teście BAPCoMobileMark® 2014 oraz czas pracy na bateriach (MobileMark 2014 Battery Runtime) wyrażony w minutach nie mniej niż 600 w teście BAPCoMobileMark® 2014 w oparciu o wyniki testów opublikowane na stronie konsorcjum BapCo - tzw. Full DisclosureReports.  2) Procesor dedykowany do rozwiązań mobilnych, energooszczędny, maksymalny współczynnik TDP (współczynnik znamionowej mocy termicznej): 15W.  3) Wydajność zaoferowanego procesora minimu 5500 pkt. na podstawie informacji uzyskanych w teście PassMark CPU Performance. Test w kolumnie PassMark CPU Mark według wyników testów procesorów opublikowanych na stronie:  1. http://www.cpubenchmark.net/cpu\_list.php.  Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie: http://www.cpubenchmark.net/cpu\_list.php w dniu wysłania do Dziennika Urzędowego Unii Europejskiej ogłoszenia o zamówieniu. |
| 2. | Przekątna i rozdzielczość ekranu | Matryca min. 14”:  1) z podświetleniem w technologii LED, powłoka antyrefleksyjna, matowa  2) rozdzielczość FHD 1920x1080,  3) kąt otwarcia matrycy min.180 stopni. |
| 3. | Pamięć RAM | Minimum 8GB z możliwością rozbudowy do 32GB, Komputer wyposażony w minimum dwa  banki pamięci umożliwiające pracę w trybie dual-channel. |
| 4. | Pamięć masowa | Minimum 240GB SSD M2, zawierający partycję RECOVERY umożliwiającą odtworzenie  systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| 5. | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną  na potrzeby grafiki. |
| 6. | Komunikacja | 1) Wbudowana karta sieci bezprzewodowej WiFi 802.11 b/g/n/ac  2) Zintegrowana karta sieciowa min. 1GBE LAN (RJ45). |
| 7. | Bezpieczeństwo | 1) Laptop musi posiadać opcję zastosowania mechanicznego zabezpieczenia przed  kradzieżą komputera.  2) Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia  i zarządzania wygenerowanymi przez komputer kluczami szyfrowania.  Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów  przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej  TPM 2.0. |
| 8. | Multimedia | Wyposażenie multimedialne:  1) karta dźwiękowa zintegrowana z płytą główną, obsługująca dźwięk stereo,  2) wbudowane dwa głośniki,    Strona 25 z 90  3) cyfrowy mikrofon wbudowany w obudowie matrycy,  4) kamera internetowa HD wbudowana w obudowie matrycy  5) napęd DVDRW producenta oferowanego komputera przenośnego z dołączonym  oprogramowaniem do nagrywania i odtwarzania. |
| 9. | Klawiatura i mysz | 1) Klawiatura wyspowa układ US –QWERTY odporna na zachlapanie, Podświetlenie  klawiatury. touchpad z obsługą gestów.  2) Mysz laserowa z rolką min. 2 przyciski, bezprzewodowa, dołączone baterie zasilające. |
| 10. | Bateria i zasilanie | Dedykowany przez producenta komputera zasilacz sieciowy, bateria min. 3 celowa. |
| 11. | Waga oraz wymiary laptopa z zaoferowanym akumulatorem | 1) Waga do 2,2kg.  2) Grubość nie przekraczająca 24 mm. |
| 12. | Obudowa | 1) Laptop wykonany z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją.  2) Laptop w czasie pracy nie może generować hałasu przekraczającego 22dB(A) deklarowanego zgodnie z obowiązującymi normami ISO 9296 oraz mierzonego wg  ISO 7779:2010 w pozycji „Operatora” (osoby obsługującej) w trybie bezczynności bez napędu optycznego i dysku HDD (IDLE). |
| 13. | Certyfikaty i oświadczenia | 1) Oferowane laptopy muszą posiadać europejską deklarację zgodności CE.  2) Producent laptopa musi posiadać ISO 9001 co najmniej w zakresie projektowania, produkcji i serwisu komputerów - oświadczenie zawarte w Formularzu ofertowym.  3) Producent laptopa musi posiadać ISO 14001 co najmniej w zakresie projektowania, produkcji – oświadczenie zawarte w Formularzu ofertowym  4) Oferowane laptopy muszą posiadać certyfikat TCO lub równoważny\* – obecność modelu na stronie https://tcocertified.com/product-finder/.- oświadczenie zawarte  w Formularzu ofertowym.  5) Oferowane modele laptopów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 lub w przypadku zaoferowania komputerów z systemem równoważnym  muszą posiadać certyfikat zgodności z zainstalowanym systemem operacyjnym. |
| 14. | BIOS | Minimalna funkcjonalność:  1) konfiguracja hasła użytkownika i administratora,  2) blokada portów USB,  3) blokada uruchamiania komputera z wybranych napędów,  4) fabrycznie wpisany nieusuwalny numer seryjny producenta |
| 15. | System operacyjny | Zainstalowany system operacyjny co najmniej Windows 10 Professional 64 bitowyw polskiej wersji językowej lub system równoważny. Klucz licencyjny systemu musi być zapisany trwale  w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.  System równoważny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1) Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.  2) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim;  3) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  4) Wbudowany system pomocy w języku polskim;  5) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim;  6) Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego;  7) Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  8) Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz  mechanizmem sprawdzającym, które z poprawek są potrzebne;  9) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego;  10) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego;  11) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  12) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,  13) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);  14) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  15) Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  16) Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  17) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe;  18) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  19) Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu;  20) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  21) Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  22) Obsługa standardu NFC (near field communication);  23) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  24) Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  25) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  26) Mechanizmy logowania do domeny w oparciu o:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  27) Mechanizmy wieloelementowego uwierzytelniania.  28) Wsparcie dla uwierzytelniania na bazie Kerberos v. 5;  29) Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,  30) Wsparcie dla algorytmów Suite B (RFC 4869);  31) Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla  warstwy transportowej IPsec;  32) Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  33) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  34) Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  35) Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;  36) Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową;  37) Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  38) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający  tworzyć kopie zapasowe;  39) Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  40) Udostępnianie modemu;  41) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  42) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci;  43) Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa  (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  44) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  45) Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,  46) Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika;  47) Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform  Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB;  48) Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych;  49) Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych; |
| 16. | Wbudowane porty i złącza | 1) minimum 2xUSB 3.1 Gen 1 (jeden z możliwością ładowania urządzeń zewnętrznych  poprzez port USB przy wyłączonym laptopie),  2) minimum 1x USB-C 3.1,  3) złącze słuchawek i mikrofonu (combo),  4) minimum 1 złącze wideo HDMI 1.4b lub DP,  5) minimum. 1 x RJ-45,  6) czytnik kart multimedialnych,  7) wbudowany w obudowie laptopa czytnik Smart card reader,  8) złącze umożliwiające podpięcie linki antykradzieżowej. |
| 17. | Wymagania dodatkowe: | Torba dopasowana i przeznaczona do oferowanego notebooka.  Torba musi spełniać poniższe warunki:  1) minimum 1 komora oraz kieszeń z przodu na akcesoria,  2) wykonana z poliestru lub nylonu,  3) musi posiadać regulowany pasek na ramię,  4) wyłożona pianką zabezpieczającą sprzęt przed uszkodzeniem,  Musi posiadać europejską deklarację zgodności CE. |
| 18. | Oprogramowanie biurowe | Równoważność dla MS Office Dla użytkowników domowych i małych firm.  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:  a) Edytor tekstów  b) Arkusz kalkulacyjny  c) Narzędzie do przygotowywania i prowadzenia prezentacji  d) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)  8. 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) Wydruk dokumentów  k) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną  l) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 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 2010, 2013 i 2016.  m) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  9. 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 np.: inne arkusze kalkulacyjne  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 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 2010, 2013 i 2016.  m) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a) 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 2010, 2013 i 2016. Zapewnienie po edycji i zapisaniu danego dokumentu bezproblemową jego dalszą pracę w programach Microsoft PowerPoint 2010, 2013 i 2016.  11. 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    W szczególności Wykonawca musi zapewnić stabilność i pełną wymaganą funkcjonalność współpracy z posiadanym przez Zamawiającego następującym oprogramowaniem:  - pełną zgodność z formatami plików utworzonych za pomocą oprogramowania MS Office |
| 19. | Gwarancja | Gwarancja producenta:  1) Na okres co najmniej 36 miesięcy Door to Door lub w lokalizacji Zamawiającego jeżeli naprawa wymaga wykonania jej w miejscu instalacji. Koszt transportu do i z naprawy pokrywa Wykonawca.  2) Czas reakcji na zgłoszoną reklamację gwarancyjną do końca następnego dnia roboczego.  3) Czas naprawy od momentu zgłoszenia do 14 dni roboczych.  4) Naprawy gwarancyjne urządzeń muszą być realizowany przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta.  5) W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  6) W przypadku gdy firma serwisująca jest inna niż producent laptopa to musi ona posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje  producenta laptopa – oświadczenie zawarte w Formularzu ofertowym.  7) Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Przełączniki szkieletowe** | | |
| 1. |  | 1. Typ i liczba portów:   Minimum 24 porty 10GBaseT umieszczonych z przodu obudowy  Minimum 6 portów 40GbE QSFP+ umieszczone z przodu obudowy z możliwością wymiany na co najmniej 2 porty 100GbE QSFP28. Jeżeli wymiana wymaga dostarczenia dodatkowego modułu, musi być on dostępny i dostarczony.   1. Wbudowany, dodatkowy, dedykowany port Gigabit Ethernet SFP do zarządzania poza pasmem - out of band management 2. Wbudowany, dodatkowy, dedykowany port Gigabit Ethernet RJ45 do zarządzania poza pasmem - out of band management 3. Port konsoli RS232 ze złączem DB9 lub RJ45 oraz port konsoli USB 4. Port USB umożliwiający podłączenie pamięci zewnętrznej (niezależny od portu konsoli USB) 5. Przepustowość minimum 714 Mpps dla pakietów 64 bajtowych 6. Wydajność: minimum 960 Gbps (prędkość przełączania „wirespeed” dla każdego portu przełącznika) 7. Przełączanie w warstwie 2 i 3 modelu OSI 8. Wielkość bufora pakietów (packet buffer): minimum 12MB 9. Minimum 1GB wbudowanej pamięci typu Flash 10. Minimum 4GB pamięci operacyjnej 11. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) 12. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika (porty) do tyłu przełącznika (zasilacze). Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. 13. Dwa wbudowane (wewnętrzne, modularne) zasilacze prądu zmiennego dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. 14. Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie ze wspólnym zarządzaniem. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 430 portów 10GbE SFP+. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)). 15. Łączenie w stos z wykorzystaniem portów 10Gb, 40Gb, 100Gb i agregowanych portów 10Gb, 40Gb i 100Gb (w celu zwiększenia przepustowości w stosie) 16. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie 17. Tablica adresów MAC o wielkości minimum 200000 pozycji 18. Obsługa minimum 50000 wpisów ARP 19. Obsługa ramek Jumbo o wielkości 10kB 20. Obsługa Quality of Service 21. Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted round robin (WRR), explicit congestion notification (ECN), SP+WFQ oraz SP+WRR 22. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 23. Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ 24. Obsługa sieci VLAN opartych o adres MAC, protokół i podsieć IP 25. Obsługa IGMP v1/v2/v3, PIM-DM, PIM-SM, BIDIR-PIM, IGMP Snooping v1/v2/v3, PIM Snooping, MLD snooping v1/v2, Multicast Source Discovery Protocol (MSDP) oraz IPv6 PIM Snooping 26. Wsparcie dla FibreChannel over Ethernet (FCF/Transit/NPV) 27. Wsparcie dla Data Center Bridging (DCB):     * IEEE 802.1Qbb Priority Flow Control (PFC)     * Data Center Bridging Exchange (DCBX)     * Enhanced Transmission Selection (ETS)     * Quantized Congestion Notification (QCN) 28. Routing IPv4 – statyczny i dynamiczny (min. RIP, IS-IS, OSPF, BGP) 29. Routing IPv6 – statyczny i dynamiczny (min. RIPng, IS-ISv6, OSPFv3) 30. Obsługa ECMP (Equal Cost Multi Path) 31. Obsługa VRRP i VRRPv6 32. Obsługa Policy Base Routing (PBR) dla IPv4 i IPv6 33. Obsługa VXLAN oraz VXLAN L3 Gateway 34. Tablica routingu o pojemności co najmniej 8000 wpisów dla IPv4 i IPv6 35. Serwer DHCP, serwer DHCPv6, klient DHCP, obsługa DHCP relay, DHCP snooping 36. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.   Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia   1. Obsługa standardu 802.1p 2. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p 3. Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, remote mirroring 4. Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x 5. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS 6. Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2 7. Syslog 8. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED 9. Obsługa sFlow 10. Obsługa NETCONF 11. Obsługa zarządzania poprzez Puppet oraz Chef 12. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 13. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter 14. Obsługa Network Time Protocol (NTP) oraz Simple Network Time Protocol (SNTP) 15. Obsługa OAM (IEEE 802.3ah) 16. Obsługa CFD (IEEE 802.1ag) 17. Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python 18. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). 19. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). 20. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. 21. Wysokość w szafie 19” – 1U o głębokości maksymalnie 46 cm 22. Maksymalny pobór mocy nie większy niż 500W 23. Minimalny zakres temperatur pracy od 0°C do 45°C 24. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. 25. Minimum 3 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na wymianę na maksymalnie następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz serwisu gwarancyjnego z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu z oprogramowaniem. Wymagana jest dostępność w trybie 8x5 w godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego.   W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania   1. W ramach zrealizowanej dostawy Wykonawca wykona wdrożenie dostarczonych przełączników sieciowych i skonfiguruje do pracy w ramach istniejącej infrastruktury sieciowej Zamawiającego. Zamawiający wymaga aby Wykonawca zapewnił na czas wdrożenia inżyniera systemowego, na czas łączny 2 dni roboczych oraz przedstawił Zamawiającemu projekt wdrożenia. Na etapie zawarcia umowy Zamawiający przekaże informacje techniczne niezbędne Wykonawcy do przygotowania projektu wdrożenia |
| **Akcesoria przełączników sieciowych** | | |
| 1. |  | Zestaw modułów połączeniowych GBIC SFP+ kompatybilnych z przełącznikami wyszczególnionymi powyżej w niniejszym dokumencie |
| **Szafa Rack 47U** | | |
| 1. | Należy dostarczyć wyposażoną szafę typu Rack 47U (przeznaczone do instalacji i eksploatacji sprzętu IT). Wewnątrz szafy zainstalowana będzie 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 zalecane jest zastosowanie wszystkich wymienionych niżej urządzeń produkowanych przez jednego producenta:  - urządzenia chłodnicze, parowniki, zintegrowane w szafie 19” w układzie zamkniętym, chłodzenie w sposób neutralny dla temp. powietrza w pomieszczeniu  - skraplacze zewnętrzne  - szafy 19” IT  - urządzenia gaśnicze wraz z wczesną detekcją pożaru  - system zdalnego monitoringu warunków środowiskowych | |
|  | Urządzenia chłodnicze zintegrowane w szafie | |
| 1. | Wymaganie minimalne | Klimatyzator typu split DX o mocy 6,5 kW składający się z jednostki wewnętrznej (parownik) i jednej jednostki zewnętrznej (chłodziarki z regulacją inwerterową). Konstrukcja jednostki wewnętrznej umożliwia zainstalowanie w szafie IT o szerokości 800 mm, jest 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 zasysa ciepłe powietrze wylotowe z serwerów bezpośrednio w tylnej części szafy i schłodzone wydmuchuje po bokach przed płaszczyzną 19". Obudowa jednostki wewnętrznej jest wykonana z blachy stalowej, wewnątrz znajduje się parownik bezpośredni, wentylatory promieniowe EC, kolektor i odpływ kondensatu.  Urządzenia powinno pozwalać na montaż z lewej lub z prawej strony szafy serwerowej IT. Ponadto 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. Wchodzący w skład systemu zewnętrzny czujnik zależy umieścić przed serwerem. Jednostka zewnętrzna ze sprężarką powinna posiadać regulacją 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 zostaje przez napięcie z urządzenia zewnętrznego.  Dane techniczne:  Użytkowa moc chłodnicza 6,5 kW  Podstawa regulacji: temperatura powietrza na wlocie do serwera, ustawiona na 22°C  Zasilanie elektryczne: 230V, 1~, N, PE, 50 Hz  Zabezpieczenie: 16A  Zakres temperatur otoczenia, jedn. zewn.: -20°C do +45°C |
|  | Szafa 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.  Należy dostarczyć szafę 19” IT.  Minimalne wymagania techniczne, funkcjonalne, wyposażenia dla szaf serwerowych, sieciowych:  - Szafa IT dopuszczona przez producenta do klimatyzacji oraz wczesnego wykrywania i gaszenia pożaru tylko wewnątrz, dla układu zamkniętego, neutralny dla powietrza otoczenia serwerowni  - Szafa serwerowa, 19”, konstrukcja ramy szaf sztywna, spawana  - Wysokość zabudowy szaf serwerowych 47U, wraz z dodatkową separacją frontową strefy zimnej.  - Przednie drzwi przeszklone o szczelności IP55 (szkło bezpieczne hartowane ESG 3mm), tylne drzwi dzielone pionowo z blachy stalowej pełne. Płyta dachu pełna.  - 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.  - Łączna obciążalność obu płaszczyzn montażowych 19” min. 1500 kg. Obciążalność szafy potwierdzona odpowiednim dokumentem.  - 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.  - Szyny profilowe 19” z przodu muszą być przygotowane do beznarzędziowego montażu elementów ułatwiających prowadzenie kabli i organizowania struktury okablowania o maksymalnej gęstości upakowania.  - 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.  - Akcesoria montażowe 19“ i kompletny zestaw uziemienia dołączone do zestawu  - Szafę należy dodatkowo wyposażyć 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.  Materiał:  – Blacha stalowa,  – Tworzywo sztuczne,  – Powierzchnia: lakierowana.  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  Dla zaślepienia wolnej przestrzeni należy z szafą dostarczyć panele zaślepiające o wysokości min. 9U przeznaczone do beznarzędziowego montażu w 19”. Panel zaślepiające mają zapewnić odpowiednie prowadzenie powietrza oraz zapewnić właściwy sposób rozprowadzenia gazu gaśniczego. Każdy panel posiada: odporność ogniową według UL 94 HB i jest samogasnący, możliwość indywidualnego dopasowania wielkości przez wyłamanie wytłaczanych elementów 1U  Dodatkowo szafa powinna zostać wyposażona w min. jeden poziomy panel porządkujący 1U wraz z wieszakami stalowymi.  Szafa dostarczona zostanie wraz z dwoma zintegrowanymi listwami zasilania PDU, opomiarowane na każdą z faz z podłączeniem do sieci zdalnego monitorowania. Przewidziano tym samym dwa tory prądowe dla szafy. Listwy PDU posiadają możliwość montażu w sposób beznarzędziowy w przestrzeni pomiędzy ścianą boczną a profilem 19” z dwoma bliźniaczymi listwami. Dla szafy zastosowano listwę PDU o max. prądzie 1x 32A.  Szafa wyposażona jest w zintegrowany system wczesnego wykrywania i gaszenia pożaru panelem gaśniczymi o wysokości montażowej max. 1U. Zastosowane urządzenie 1U posiada wew. zintegrowany pojemnik zawierający środek gaśniczy dla kubatury min. 2,8 m3. Środek gaśniczy nie stanowi żadnego ryzyka dla ludzi przebywających w pomieszczeniu, do którego wyzwalany jest środek w stężeniu gaśniczym. Projektowany środek gaśniczy wyzwalany jest 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. Detekcja pożaru następuje poprzez dwie czujki pożaru zintegrowane w panelu gaśniczym, powietrze z wnętrza szafy zasysane jest i analizowane poprzez system dedykowanej instalacji. Informacje o alarmach, awariach, ostrzeżenia, wymaganej konserwacji przesyłane są do systemu monitorowania warunków środowiskowych. Panel gaśniczy posiada niezależne zintegrowane zasilanie awaryjne na czas min. 4 godz.  Szafa 19” wyposażona jest w czujniki otwarcia drzwi przednich i tylnych monitorujące ich otwarcie oraz rozbrojenie systemu gaszenia na czas otwarcia drzwi. |
|  | Opis technologiczny PDU | |
| 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) | 24 |
| 5. | Liczba gniazdek typu EN60320/C13 (na fazę / bezpiecznik) | 12 |
| 6. | Liczba gniazdek typu EN60320/C19 (łącznie) | 4 |
| 7. | Liczba gniazdek typu EN60320/C19 (na fazę / bezpiecznik) | 2 |
| 8. | Liczba wyłączników ochronnych | 2 |
| 9. | Liczba elektromagnetycznych wyłączników ochronnych | 16A Typ C |
| 10. | Wtyk przyłączeniowy wejścia PDU | EN60309 / CEE |
| 11. | Długość kabla przyłączeniowego | 3m |
| 12. | Typ kabla przyłączeniowego | H05-VV |
| 13. | Liczba żył | 3 |
| 14. | Przekrój kabla | 4mm² |
| 15. | Funkcje pomiaru | Pomiar dla każdej fazy lub zasilania |
| 16. | Rejestrowane wartości (na fazę) | Napięcie (V), prąd (A), częstotliwość (Hz) |
| 17. | Zakres pomiaru napięcia | 90V- 260V |
| 18. | Konfigurowalne wartości graniczne (ostrzeżenie/alarm) | Tak |
| 19. | Licznik godzin pracy | Tak |
| 20. | Wyświetlacz / wskaźniki | OLED, RGB 128x128 pikseli |
| 21. | Interfejs sieciowy | RJ45, zintegrowany websewer |
| 22. | Obsługiwane protokoły | |  | | --- | | HTTP, HTTPS, SSL, SSH, NTP, Telnet | | TCP/IP v4 i v6, DHCP, DNS, NTP, Syslog | | SNMP v1, v2c i v3, XML | | FTP/SFTP (aktualizacja / transfer plików) | | Wysyłanie e-maili (SMTP) | |
| 23. | Administrowanie użytkownikami i uprawnieniami | Tak |
| 24. | Typy czujników CAN | Temperatura, temperatura i wilgotność (kombi), czujnik dostępu IR, czujnik wandalizmu |
| 25. | Zgodność | CE |
| 26. | Bezpieczeństwo | PN-EN 60950-1 |
| 27. | EMC | |  | | --- | | PN-EN 61000-4-2 | | PN-EN 61000-4-3 | | PN-EN 61000-6-2 | | PN-EN 61000-6-3 | |
| 28. | Dyrektywa bezpieczeństwa | 2014/35/EU |
| 29 | Dyrektywa EMC | 2014/30/EU |
| 30. | Stopień ochrony | IP 20 (PN-EN 60529) |
| 31. | Parametry środowiskowe | RoHS |
| 32. | Temperatury otoczenia | 0°C do +45°C |
| 33. | Wilgotność otoczenia | 10 - 95% wilg. wzgl., brak kondensacji |
|  | System monitorowania warunków środowiskowych | |
| 1. | Wymagania minimalne | Dla poprawnego działania dostarczonego systemu chłodzenia szafy IT oraz systemu gaszenia należy zastosować system zdalnego monitorowania warunków fizycznych. System ten powinien być w pełni kompatybilny z funkcjonalnością dostarczonego urządzenia gaśniczego, chłodniczego oraz szafy IT. System oparty o centralną jednostkę sterującą posiadającą jeden adres IP, do której będzie można podłączyć min. 32 czujniki, elementy. Jednostka centralna może być podłączona przez Ethernet do sieci danych, konfigurowane przez Web / USB, wysyłać alarmy przez serwer poczty elektronicznej oraz Moduł GSM. Moduł GSM dla komunikacji SMS musi obsługiwać zakresy częstotliwości dla zakresu do 4G włącznie. Dodatkowo powinna istnieć możliwość przesyłania powiadomień alarmowych z mini. 4 innych Modułów zarządzających spiętych w jedna sieć komunikacyjną.  - Obsługiwane protokoły: TCP/IPv4, TCP/IPv6, SNMPv1, SNMPv2c, SNMPv3, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS, SMTP, Syslog, LDAP, Modbus TCP IP.  - Zintegrowany WEB serwer  -Zintegrowany serwer posiadający OPC UA, uniwersalny przemysłowy protokół komunikacyjny umożliwiający komunikację pomiędzy urządzeniami, odczytywanie danych z czujników przez system nadrzędnego sterowania  - Port szeregowy komunikacyjny RS232  - 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  - Równoległa do SNMP możliwość komunikacyjna centralnego modułu monitorowania protokołem Modbus TCP IP  - Stopień ochrony modułów monitoringu: min IP 30 wg PN-EN 60 529  - Maks. łączna długość przewodów dla magistrali CAN-Bus w jednym module: 100m  - Obsługa zasilania redundantnego dla modułu centralnego monitoring POE - Power over Ethernet  - Zegar czasu rzeczywistego z NTP z buforem energii (24h) bez baterii/akumulatora  - Zarządzanie użytkownikami: LDAP  Do zastosowanego systemu zdalnego monitoringu i zarządzania pracą urządzenia gaśniczego, urządzenia chłodniczego, dodatkowo należy zastosować w szafie 19” IT min. 1 czujnik dualny temperatura-wilgotności, czujnik wycieku punktowy oraz Moduł wejścia – wyjścia dla sygnałów bez potencjałowych.  Czujnik dualny temperatura-wilgotność. Zakres pomiarowy temp.: 0°C…+55°C, dokładność pomiaru +- 1K, rozdzielczość pomiaru zmiany temp. 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.  Moduł Wejścia-Wyjścia. Monitorowanie maksymalnie ośmiu wejść cyfrowych i sterowanie za pomocą maksymalnie czterech wyjść przekaźnikowych. W programie istnieje możliwość połączenia przekaźników i wartości pomiarowych w taki sposób, aby załączały się w określonych okolicznościach. W ten sposób można kontrolować urządzenia lub przekazywać komunikaty. Szybkie podłączenie automatyczne rozpoznawanie przez plug &play. Małe zapotrzebowanie na miejsce dzięki dużej koncentracji wejść i wyjść.  Zakres temperatury pracy: 0°C…+45°C |
|  | System automatycznego awaryjnego otwarcia drzwi szafy | |
| 1. | Wymagania minimalne | Szafa wyposażona w zintegrowany system awaryjnego automatycznego otwarcia drzwi przednich i tylnych. Zadaniem automatyki systemu jest otwarcie drzwi szaf w sposób automatyczny w przypadku braku zasilania oraz awarii układu chłodzenia od ustawionego wzrostu temp. wewnątrz zamkniętej szafy. Szaf została 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 została 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. Modułów sterujący zainstalowany w szafie posiada : 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. Dodatkowo system wyposażony jest w sterownik plug & play dla integracji z opcjonalnym oprogramowaniem DCIM Software. System automatycznego awaryjnego otwarcia drzwi szafy umożliwia integrację oraz współpracę automatyki z zaprojektowanym wymiennikiem DX. System umożliwia zdalną konfigurację standardowo poprzez Web interfejs oraz opcjonalnie przez oprogramowanie DCIM. |
|  | Wymagania w zakresie instalacji i konfiguracji | |
| 11. |  | Montaż i posadowienie szafy na potrzeby środowiska przetwarzania danych w pomieszczeniu udostępnionym przez Zamawiającego. |
| 12. |  | Podłączenie listew zasilających PDU w szafie do instalacji elektrycznej udostępnionej przez Zamawiającego poprzez zasilacz awaryjny UPS. |
| **System klasy DLP** | | |
| 1. | Wymagania minimalne | Ochrona przed wyciekiem danych   1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8/Windows 8.1/ Windows 10. 2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019. 3. Wsparcie dla 32 i 64-bitowej wersji systemu Windows. 4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim. 5. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim. 6. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL. 7. Serwer administracyjny musi działać w architekturze klient-serwer, gdzie komunikacja pomiędzy serwerem zarządzającym a klientem odbywa się przy pomocy agenta. 8. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 9. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych. 10. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem a serwerem zarządzającym. 11. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym. 12. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol. 13. Administrator musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z usługą Active Directory. 14. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych, kopia ustawień serwera. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące. 15. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania. 16. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu, jak i ich usuwania oraz klonowania. 17. Administrator musi mieć możliwość synchronizacji grup administratorów konsoli DLP z grupami zabezpieczeń Active Directory. 18. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na moduły odpowiadające poniższym funkcjonalnościom:     1. Monitorowania: wykorzystywanych aplikacji, odwiedzanych stron internetowych, wykorzystywanych plików, podłączonych urządzeń zewnętrznych oraz przesłanych i odebranych wiadomości e-mail;     2. DLP: służące do oznaczania plików, tworzenia reguł wykorzystania plików wrażliwych, białych i czarnych list urządzeń;     3. Nadzorcy: Kontroli dostępu do stron internetowych, kontroli dostępu do aplikacji oraz kontroli dostępu do druku. 19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą a serwerem, w czasie rzeczywistym. 20. Serwer administracyjny musi umożliwiać zablokowanie uruchomienia trybu awaryjnego na stacji końcowej. 21. Serwer administracyjny musi mieć możliwość ustawień powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanych z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji. 22. Administrator musi mieć możliwość ustawienia, godzin w których nie będą obowiązywały użytkowników reguły kontroli aplikacji oraz stron internetowych. 23. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach. 24. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS. 25. Konsola musi posiadać możliwość wysyłania alarmów dotyczących incydentów bezpieczeństwa. 26. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu. 27. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach. 28. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu. 29. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail. 30. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania. 31. Serwer administracyjny musi umożliwiać tagowanie plików na poziomie systemu plików lub na poziomie metadanych pliku. 32. Serwer administracyjny musi umożliwiać wykonanie zadania tagowania plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie istniejących plików z tagami. 33. Serwer administracyjny musi mieć możliwość tagowania plików wrażliwych w oparciu o: 34. aplikacje, z której zostały utworzone, 35. lokalizację, 36. adres URL, 37. format pliku, 38. zawartość pliku. 39. Dla plików, które zostały otagowane, musi być możliwe utworzenie następujących reguł: 40. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na dyskach lokalnych lub określonych, 41. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń, 42. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach, 43. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej, 44. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen. 45. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do folderów synchronizacji z usługami chmury, 46. blokowanie oraz zezwalanie na zapisywanie i przenoszenie poprzez usługę pulpitu zdalnego, 47. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty oraz wirtualnego drukowania, 48. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje. 49. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizyczne i sieciowe, lokalizacje sieciowe, adresy e-mail oraz domeny, urządzenia przenośne, FireWire oraz Bluetooth, które mogą być wykorzystywane do określenia reguł dostępu. 50. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury. 51. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń FireWire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT. 52. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM. 53. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika. 54. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych. 55. Serwer administracyjny musi posiadać możliwość blokowania stron internetowych w oparciu o kategorię stron oraz adres URL. Musi istnieć możliwość konfiguracji przekierowania z dowolnej strony, która została zablokowana. 56. Serwer administracyjny musi posiadać możliwość blokowania aplikacji w oparciu o jej kategorię, lokalizację oraz źródło pochodzenia (np. Sklep Windows). 57. Serwer administracyjny musi posiadać możliwość blokowania drukowania na wszystkich lub określonych drukarkach fizycznych, sieciowych oraz wirtualnych. Musi także posiadać możliwość określenia limitu drukowanych stron w ciągu dnia, tygodnia lub miesiąca. 58. Serwer administracyjny musi posiadać możliwość tagowania plików w oparciu o ich zawartość, co najmniej o: 59. numery kart kredytowych, 60. numer PESEL, 61. numer polskiego dowodu osobistego, 62. wyrażenia regularne, 63. określone ciągi znaków, 64. numer IBAN. 65. Weryfikacja zawartości pliku powinna odbywać się w czasie rzeczywistym. 66. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie tagowania. 67. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate. 68. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM. 69. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików. 70. Serwer administracyjny musi umożliwiać import niestandardowych dzienników dla klasyfikacji zawartości dokumentów. 71. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi. 72. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu, które są podzielone na: 73. Bezpieczeństwo danych:     * + Przegląd informacji o incydentach bezpieczeństwa.       + Przegląd danych przychodzących.       + Przegląd danych wychodzących.       + Przegląd informacji z Office365, które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.       + Podłączane/odłączane urządzenia przenośne. 74. Produktywność:     * + Przegląd informacji na temat produktywności użytkowników.       + Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.       + Trendy. 75. Eksploatacja sprzętu:     * + Przegląd informacji na temat eksploatacji sprzętu komputerowego.       + Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.       + Eksploatacja drukarek.       + Eksploatacji sieci. 76. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP. 77. W konsoli webowej musi istnieć możliwość konfiguracji połączenia z Office 365. 78. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania. 79. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje na temat:     * + plików przenoszonych na nośniki USB i inne urządzenia przenośne,       + plików przesłanych za pomocą wiadomości e-mail,       + plików przesłanych za pomocą poczty webowej,       + plików przesłanych do Internetu,       + plików wysłanych za pomocą komunikatorów,       + plików przesłanych na dyski chmurowe,       + analiza sposobu korzystania z aplikacji,       + analiza korzystania z Internetu,       + analiza wykorzystania portali do poszukiwania pracy. 80. W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania. Wykonawca dostarczy i skonfiguruje system NAC po wcześniejszym uzgodnieniu z Zamawiającym projektu wdrożenia |
| **System klasy NAC (Network Access Control)** | | |
| 1. | Wymagania minimalne | System do kontroli dostępu musi charakteryzować się następującymi cechami:   * Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor) * System musi odsługiwać minimum 300 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia * Praca jako maszyna wirtualna * Musi posiadać wbudowany serwer Radius * Musi posiadać wbudowany serwer TACACS+ (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie) * Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:   + Cisco Systems   + Fortinet   + Microsoft   + Alcatel-lucent Enterprise   + Aruba Networks   + Huawei   + Extreme Networks   + PaloAlto * System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera * System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. * Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych. * Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych   + Microsoft Active Directory   + Radius   + Kerberos   + LDAP   + ODBC   + Współpraca z serwerami tokenów * Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie):   + DHCP   + TCP   + MAC OUI   + SNMP   + Cisco device sensor * Wspierać protokoły   + Radius, Radius CoA, TACACS +, web authentication, SAML v2.0   + EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)   + PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)   + TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)   + EAP-TLS   + PAP, CHAP, MSCHAPv1 i v2, EAP-MD5   + NAC, Microsoft NAP   + Windows machine authentication   + MAC Auth   + Audit (role oparte na porcie oraz skanowanie podatności)   + OCSP (Online Certificate Status Protocol)   + SNMP generic MIB, SNMP private MIB   + CEF (Common Event Format), LEEF (Log Event Extended Format)   + TLS 1.2 * Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie) * Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:   + Co najmniej ESX 4.0, ESXi 4.1 do 6.0   + Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise   - Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (300). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.  System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności   * Samodzielna rejestracja klientów gościnnych w oparciu o:   + Adres e-mail   + Numer telefonu (wiadomość SMS)   + Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link) * Logowanie w oparciu o portale społecznościowe * Funkcja integracji z systemami trzecimi poprzez API * Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową * Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych. * Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych. * Funkcja personalizacji strony gościnnej   - Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.   * Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT * System musi wspierać obsługę następujących systemów operacyjnych   + MS Windows   + Mac OS X   + iOS   + Android   + Chromebook   + Ubuntu * Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci * Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej * Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu. * Funkcja tworzenia unikalnych certyfikatów dla urządzeń. * Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń * Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID   - Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.  System kontroli końcówek klienckich musi mieć następujące funkcjonalności   * System musi wspierać następujące systemy operacyjne   + Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)   + Apple Mac OS X 10.7 i nowsze   + Red HAT Enterprise Linux 4 i nowsze   + CentOS 4 (Community Enterprise Operating System) i nowsze   + Fedora Core 5 i nowsze   + SUSE linux 10.x i nowsze * Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall * Wyświetlanie informacji on-line o statusie monitorowanych końcówek * System powinien obsługiwać agenta w formie   + Stałej (Presistent Agent)   + Tymczasowej (Dissolvabe Agent)   + Agenta NAP |
| 2. | Gwarancja | Minimum 3 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.  - Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.  - Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu  - Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.  W ramach zrealizowanej dostawy, Wykonawca musi zapewnić usługi gwarancyjne zapewniające możliwość zgłoszenia i rozwiązania bieżących problemów oraz incydentów technicznych związanych z użytkowaną infrastrukturą i oprogramowaniem dostarczonymi w ramach niniejszego postępowania |
| Urządzenia wielofunkcyjne | | |
|  | Wymagania minimalne | TYP URZĄDZENIA - Fabrycznie nowe monochromatyczne urządzenie wielofunkcyjne formatu A4, gotowe do pracy   * PRĘDKOŚĆ KOPIOWANIA – min 50 stron na minutę * PANEL OPERACYJNY - min 10 cali * DYSK TWARDY – min 320 GB * PAMIĘĆ RAM – min 2 GB * INTERFEJSY - Ethernet BASE 10/100/1000, USB 2.0 * POJEMNOŚĆ WEJŚCIOWA PAPIERU - 600 arkuszy * POJEMNOŚĆ WYJŚCIOWA PAPIERU - 500 arkuszy * OBSŁUGIWANE SYSTEMY OPERACYJNE - Windows 10, Windows Server 2008, Windows Server 2008R2, Macintosh OS X Native v10.11 lub późniejszy * MODUŁ SKANERA – Skaner z szybą ekspozycyjną oraz jednoprzebiegowym podajnikiem oryginałów * PRĘDKOŚĆ SKANOWANIA – min 60 obrazów mono A4 na minutę * DOCELOWE FORMATY SKANOWANYCH DOKUMENTÓW - PDF, archiwalny PDF, PDF zabezpieczony hasłem, PDF z podpisem elektronicznym * DOCELOWE LOKALIZACJE ZAPISU SKANOWANYCH DOKUMENTÓW - Foldery sieciowe, poczta e-mail, USB, Karta SD * OBSŁUGIWANE FORMATY PAPIERU - Minimum A4, A5, A6, B5, B6 * OBSŁUGIWANA GRAMATURA PAPIERU - Minimum 60 - 200 g/m² * JĘZYKI DRUKARKI – PCL5e, PostScript 3 * MAKSYMALNE ZUŻYCIE ENERGII - Nie większe niż 1,5 kW * MATERIAŁY EKSPLOATACYJNE - Urządzenie w standardzie musi posiadać materiały eksploatacyjne o wydajności przynajmniej: - dla tonera: 10 tys. wydruków  - dla bębnów światłoczułych: 500 tys. wydruków Wydajność ma być zgodna z deklaracjami producenta w jego oficjalnej dokumentacji. W przypadku niespełnienia wymogów wydajnościowych Zamawiający zaakceptuje równoważną ilość materiałów (np. dodatkowy komplet tonerów). * PODSTAWA - Nie wymagana * INSTALACJA - W ramach realizacji zamówienia Wykonawca dostarczy, uruchomi i zainstaluje urządzenia w sieci komputerowej Zamawiającego oraz przeprowadzi integrację dostarczonego sprzętu z systemem archiwizacji i zasilania szpitalnej bazy danych EDM cyfrową wersją dokumentacji medycznej wytworzonej w postaci papierowej * UWAGI - W każdym punkcie, w którym pojawiają się wymogi dotyczące prędkości i pojemności Zamawiający oczekuje parametrów dla typowego papieru biurowego, niepowlekanego, o gramaturze 80 g/m². Zamawiający zaakceptuje tylko te parametry, które można potwierdzić w oficjalnych źródłach informacji o produkcie tzn. strona internetowa producenta, broszura produktowa, katalog produktowy, specyfikacja techniczna. |
|  | Gwarancja | Gwarancja jakości producenta:  1) Na okres co najmniej 36 miesięcy Door to Door lub w lokalizacji Zamawiającego jeżeli naprawa wymaga wykonania jej w miejscu instalacji. Koszt transportu do i z naprawy pokrywa Wykonawca.  2) Czas reakcji na zgłoszoną reklamację gwarancyjną do końca następnego dnia roboczego.  3) Czas naprawy od momentu zgłoszenia do 14 dni roboczych.  4) Naprawy gwarancyjne urządzeń muszą być realizowany przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta.  5) W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  6) W przypadku gdy firma serwisująca jest inna niż producent urządzenia wielofunkcyjnego to musi ona posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzenia wielofunkcyjnego – oświadczenie zawarte w Formularzu ofertowym.  7) Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
|  |  |  |

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.