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

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

**dla Instytutu Matki i Dziecka w Warszawie**

# 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** | 4 |
|  | **Macierz dyskowa** | 2 |
|  | **Przełącznik dystrybucyjny** | 2 |
|  | **UTM** | 2 |
|  | **Komputer stacjonarny** | 90 |
|  | **Laptop** | 60 |
|  | **Tablet** | 60 |
|  | **UPS** | 4 |
|  | **Oprogramowanie backupowe** | 1 |
|  | **Oprogramowanie wirtualizacyjne** | 4 |
|  | **Licencje systemów operacyjnych** | 4 |
|  | **Oprogramowanie bazodanowe** | 4 |

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** | | |
|  | Obudowa | Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
|  | Płyta główna | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
|  | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
|  | Procesor | Zainstalowane dwa procesory min. 16-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 176 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla dwóch procesorów. |
|  | RAM | Minimum 256 DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się min. 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać co najmniej 3TB pamięci RAM. |
|  | Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling |
|  | Gniazda PCI | - minimum dwa sloty PCIe x16 generacji 3 połowy wysokości |
|  | Interfejsy sieciowe/FC/SAS | Wbudowane min. dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT.  Możliwość instalacji wymiennie modułów udostępniających:  - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT,  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+,  - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+,  - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.  Dodatkowa karta sieciowa 2x10Gb SFP+ oraz karta HBA 2x 16Gb FC. |
|  | Dyski twarde | Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.  Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID 1. |
|  | Kontroler RAID | Wbudowany kontroler SATA. |
|  | Napęd optyczny | Wewnętrzny DVD-RW SATA. |
|  | System operacyjny/wirtualizator | Zainstalowany obraz systemu VMware ESXi 6.7 U2 lub równoważnego\* na dostarczonych kartach SD. |
|  | Wbudowane porty | 4 x USB z czego nie mniej niż 1 na przednim panelu obudowy i jeden wewnętrzny, 4 x RJ-45, 2xVGA z czego jeden na panelu przednim, 1xRS-232. |
|  | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. |
|  | Wentylatory | Redundantne. |
|  | Zasilacze | Redundantne, Hot-Plug min. 750W każdy. |
|  | Bezpieczeństwo | Wbudowany moduł TPM 2.0.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
|  | Diagnostyka | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
|  | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej, * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, * możliwość podmontowania zdalnych wirtualnych napędów, * wirtualną konsolę z dostępem do myszy, klawiatury, * wsparcie dla IPv6, * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH, * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz, * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, * integracja z Active Directory, * możliwość obsługi przez ośmiu administratorów jednocześnie, * Wsparcie dla automatycznej rejestracji DNS, * wsparcie dla LLDP, * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, * możliwość podłączenia lokalnego poprzez złącze RS-232, * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy, * monitorowanie zużycia dysków SSD, * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * automatyczne zgłaszanie alertów do centrum serwisowego producenta, * automatyczne update firmware dla wszystkich komponentów serwera, * możliwość przywrócenia poprzednich wersji firmware, * możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON, * możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych, * automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. |
|  | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważnymi.  Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019. |
|  | Wspierane systemy operacyjne | Co najmniej CitriX XenServer, Microsoft Windows Server włączając Microsoft Hyper-V, Vmware vSphere, Oracle Linux i wirtualizacja, Red Hat Enterprise Linux i wirtualizacja. |
|  | Warunki gwarancji | 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnodostępne na terenie kraju narzędzie komunikacyjne zapewniające możliwość zgłoszenia awarii w systemie 24/7/365 z natychmiastowym potwierdzeniem przyjęcia zgłoszenia.  Zamawiający wymaga od podmiotu realizującego serwis 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.  Firma serwisująca musi posiadać system zarządzania jakością zgodny z ISO 9001:2008 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  .  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. |
|  | Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim w wersji elektronicznej.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Macierz dyskowa** | | |
|  | **Macierz** | Macierz powinna posiadać co najmniej dwa redundantne kontrolery macierzowe wraz z możliwością instalacji 30 dysków,  Maksymalna wysokość 3U,  Macierz musi umożliwiać rozbudowę o moduły co najmniej 12 dysków 3,5”, co najmniej o 24 dyski 2,5” i co najmniej 60 dysków 3,5”.  Obsługa min. 222 dysków SAS/NLSAS lub SSD.  Macierz powinna posiadać co najmniej dwa kontrolery w jednej obudowie. |
|  | **Wymagana przestrzeń** | Macierz musi być wyposażona w:   * Min. 14 dysków 2,5” o pojemności co najmniej 1.8TB 10k, SAS 12Gb/s, * Min. 6 dysków 2,5” o pojemności co najmniej 960GB SSD RI SAS 12Gb/s. |
|  | **Pamięć podręczna (Cache)** | Pamięć podręczna (cache) – 16 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 32 GB).  Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash.  W przypadku awarii podtrzymanie zawartości pamięci cache przez min. 96 h. |
|  | **Interfejsy zewnętrzne** | Macierz musi być wyposażona w 8 portów FC 16Gb, 2 porty zarządzające 1GbE Base-T, każdy kontroler macierzy w trybie Active-Active. Dodatkowo należy dostarczyć 4 kable LC-LC o długości min. 3m. |
|  | **Dostępność** | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).  Możliwość łączenia w macierzy różnych poziomów RAID:   * możliwość zastosowania RAID10, * możliwość zastosowania RAID 10DM, * możliwość zastosowania RAID5, * możliwość zastosowania RAID6, * możliwość zastosowania RAID0, * możliwość zastosowania RAID1.   Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych.  Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.  Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).  Możliwość zdefiniowania min. 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa.  Możliwość obsługi wirtualnych portów (NPIV) w taki sposób, aby awaria fizycznego portu nie powodowała konieczności przełączania ścieżek poprzez oprogramowanie do multipathing. |
|  | **Wspierane systemy operacyjne** | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej: AIX, HP-UX, MS Windows, VMware oraz Linux, APPLE IOS.  Wymagane wsparcie dla różnych systemów klastrowych, co najmniej: Veritas Cluster Server, HACMP, HP Serviceguard.  Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: AIX, HP-UX, MS Windows, Vmware, Linux.  Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning. |
|  | **Skalowalność** | Wykonywanie rozbudowy sprzętowej w trybie online.  Umożliwia rozbudowę do minimum 222 dysków 2,5”.  Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu.  Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej. |
|  | **Zarządzanie** | Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).  Stałe monitorowanie macierzy przez zdalne centrum serwisowe.  Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów.  Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych.  Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej 500TB.  Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
|  | **Możliwość migracji danych w obrębie macierzy** | Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków oraz rożnymi poziomami RAID w zależności od stopnia obciążenia macierzy dyskowej. Dane często używane macierz powinny automatycznie przemieszczać na dyski o największej prędkości obrotowej, dane rzadko używane na dyski o prędkości obrotowej 7200 rpm. Dodatkowo funkcjonalność ta musi wspierać dyski SSD zoptymalizowane przez producenta dysków do zapisu lub do odczytu.  Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie.  Macierz musi umożliwiać tworzenie jednego wolumenu logicznego LUN w obrębie wszystkich produkcyjnych dysków macierzy. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. Musi również umożliwiać udostępnienie tego wolumenu logicznego LUN po protokole FC. |
|  | **Lokalna replikacja danych** | Możliwość tworzenia kopii danych z poziomu macierzy i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.  Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora.  Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej.  Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot.  Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write).  Kopie migawkowe muszą mieć możliwość prezentacji jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ja dostarczyć. |
|  | **Redukcja danych** | Macierz powinna zapewniać metody redukcji ilości danych blokowych za pomocą kompresji. Kompresja powinna odbywać się po fakcie zapisu na urządzenia dyskowe wewnątrz macierzy (dane spoczynkowe). |
|  | **Kontrola przepływu danych - QoS** | Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych wolumenów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie. |
|  | **Współpraca z aplikacjami** | Możliwość integracji środowiska VMware, Microsoft SQL z mechanizmem lokalnej replikacji danych. |
|  | **Importowanie danych** | Macierz musi posiadać funkcjonalność onlinowego importu danych z macierzy innego producenta z jednoczesną konwersją wolumenu logicznego LUN do trybu „Thin Provision”. |
|  | **Gwarancja** | Min. 36 miesięcy gwarancji z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dysków pozostają one własnością Zamawiającego.  Oświadczenie producenta serwera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisie. |
|  | **Wymiana dysków** | Wymiana dysków może być dokonywana przez klienta. |
| **Przełącznik dystrybucyjny** | | |
|  | **Porty** | Przełącznik 1U wyposażony w porty:   * 48 portów 100M/1G/10G Ethernet RJ 45, * 4 portów 10 Gigabit Ethernet QSFP+, * port konsoli i port zarządzania out of band management, * 1 port USB 2.0 type A, * 1 port Micro-USB 2.0 type B. |
|  | **Przepustowość** | Przepustowość zagregowana minimum 1080Mpps. |
|  | **System operacyjny** | Modularny system operacyjny.  Musi umożliwiać instalacje różnych systemów operacyjnych wspieranych przez producenta w celu uzyskania dodatkowych funkcjonalności zgodnie z rekomendacją SDN. |
|  | **Zasilanie** | Nadmiarowy zasilacz AC (hot-swapable).  Max. konsumpcja mocy: 420 Watt. |
|  | **RACK** | Musi zapewniać instalację w szafach 19”. |
|  | **Pamięć** | Moduł pamięci SSD: 8 GB.  Pamięć CPU: 4GB.  Pojemność bufora pakietów: 16MB. |
|  | **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 1.44Tbps (full-duplex).  Szybkość przełączania ramki w obrębie przełącznika maksymalnie 3 mikrosekund. |
|  | **Chłodzenie** | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne).  Musi być wyposażone w redundantne i wymienne w trakcie pracy (hot-swappable) 2 wiatraki. |
|  | **Funkcjonalności** | Musi obsługiwać ramki „Jumbo” o długości min. 11000 B.  Musi obsługiwać, co najmniej 4000 VLANów.  Pamięć, dla co najmniej 160 000 adresów MAC.  Musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+, MSTP.  Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach,  - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy, - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń,  - implementacje dedykowanego protokołu innego niż STP, RSTP, PVST+.  MSTP umożliwiający szybką konwergencję sieci w przypadku zastosowania topologii Ring.  Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG.  Musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow Control, oraz 802.1Qaz Enhanced Transmission Selection (ETS).  Musi zapewniać sprzętowe wsparcie dla L2 VXLAN oraz L3 VXLAN.  Musi obsługiwać protokół Ethernet Ring Protection Switching, (ERPS) lub równoważny.  Musi obsługiwać mechanizm BFD (Bidirectional Forwarding Detection).  **Musi obsługiwać standardy IEEE:**  802.1AB LLDP,  802.1D Bridging, STP,  802.1p L2 Prioritization,  802.1Q VLAN Tagging, Double VLAN Tagging, GVRP,  802.1X Network Access Control (Port Authentication),  802.3ab Gigabit Ethernet (1000BASE-T),  802.3ac Frame Extensions for VLAN Tagging,  802.3ad Link Aggregation with LACP,  802.3ae 10 Gigabit Ethernet (10GBASE-X),  802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4),  802.3u Fast Ethernet (100BASE-FX) on management ports,  802.3x Flow Control,  802.3z Gigabit Ethernet (1000BASE-X),  ANSI/TIA-1057 LLDP-MED.  **Musi obsługiwać, co najmniej poniższe standardy:**  768 User Datagram Protocol,  793 Transmission Control Protocol,  854 Telnet Protocol Specification,  959 File Transfer Protocol (FTP),  2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,  3164 The BSD syslog Protocol.  **RFC w zakresie protokołu IPv4:**  791 Internet Protocol,  792 Internet Control Message Protocol,  826 An Ethernet Address Resolution Protocol,  1027 Using ARP to Implement Transparent Subnet Gateways,  1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION (client),  1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks,  1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis,  1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy,  1542 Clarifications and Extensions for the Bootstrap Protocol,  1812 Requirements for IP Version 4 Routers,  1858 IP Fragment Filtering,  2131 Dynamic Host Configuration Protocol,  5798 Virtual Router Redundancy Protocol (VRRP),  3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links,  3046 DHCP Relay Agent Information Option,  3069 VLAN Aggregation for Efficient IP Address Allocation,  3128 Protection Against a Variant of the Tiny Fragment Attack.  **Musi obsługiwać, co najmniej poniższe standardy RFC w zakresie protokołu IPv6:**  1858 IP Fragment Filtering,  2460 Internet Protocol, Version 6 (IPv6) Specification,  2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,  2675 IPv6 Jumbograms,  3587 IPv6 Global Unicast Address Format,  4291 Internet Protocol Version 6 (IPv6) Addressing Architecture.  **Musi obsługiwać Multicast w tym, co najmniej poniższe standardy RFC i drafty**:  1112 Host Extensions for IP Multicasting,  2236 Internet Group Management Protocol, Version 2,  3376 Internet Group Management Protocol, Version 3,  3569 An Overview of Source-Specific Multicast (SSM),  4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches,  draft-ietf-pim-sm-v2-new-05 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised).  **Musi umożliwiać obsługę Statycznego i Dynamicznego Routingu.**  **Musi obsługiwać protokół OSPF, w tym co najmniej poniższe standardy RFC dla OSFP:**  1587 The OSPF Not-So-Stubby Area (NSSA) Option,  2154 OSPF with Digital Signatures,  2328 OSPF Version 2,  2370 The OSPF Opaque LSA Option,  2740 OSPF for IPv6,  3623 Graceful OSPF Restart,  4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance.  **Musi obsługiwać protokół BGP, w tym co najmniej poniższe standardy RFC i drafty dla BGP:**  1997 BGP Communities Attribute,  2385 Protection of BGP Sessions via the TCP MD5 Signature Option  2439 BGP Route Flap Damping,  2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing,  2796 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP),  2842 Capabilities Advertisement with BGP-4,  2858 Multiprotocol Extensions for BGP-4,  2918 Route Refresh Capability for BGP-4,  3065 Autonomous System Confederations for BGP,  4360 BGP Extended Communities Attribute,  4893 BGP Support for Four-octet AS Number Space,  5396 Textual Representation of Autonomous System (AS) Numbers,  draft-ietf-idr-bgp4-20 Border Gateway Protocol 4 (BGP-4),  draft-ietf-idr-restart-06 Graceful Restart Mechanism for BGP,  **W tym, co najmniej poniższe standardy RFC dla IS-IS**:  1195 Routing in TCP/IP and Dual Environments,  5308 Routing IPv6 with IS-IS.  **W tym, co najmniej poniższe standardy RFC dla VRF:**  4364 VRF-lite (IPv4 VRF with OSPF, BGP, IS-IS and V4 multicast).  **Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:**   * Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, * Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi, * Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), * Implementacja mechanizmu Weighted Random Early Detection (WRED), * Obsługa IP Precedence i DSCP.   **Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci:**   * co najmniej 3 poziomy dostępu administracyjnego przez konsole, * urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100/1000BaseT, * autoryzacja użytkowników/portów w oparciu o 802.1x oraz EAP * Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2, * implementacji listy kontroli dostępu (ACL) na poziomie co najmniej warstwy 2, * obsługa DHCP Snooping, * obsługa dynamicznej inspekcji ARP, * obsługa walidacji adresów IP o MAC (MAC+IP Source Address Validation), * Obsługa walidacji adresów MAC (DHCP MAC Address Validation), * obsługa, co najmniej sFlow v5 lub ekwiwalentu, * obsługa RMON, * obsługa monitorowania ruchu na porcie (Port Monitoring), * plik konfiguracyjny urządzenia musi być możliwy do edycji ‘off-line’. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzanS6000-ON, S4048-ON, S6100-ON, Z9100-ON, S6010-ON, S4048T-ON, * wymaganie spełnione. ia po dokonaniu zmian, * Urządzenie musi posiadać funkcjonalność automatycznej konfiguracji poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware) i pliku konfiguracyjnego w trakcie pierwszego podłączenia do sieci Ethernet, * Musi obsługiwać RestAPI oraz posiadac wsparcie dla Ansible. |
|  | **Gwarancja** | 3 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do końca następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. |
|  | **Dokumentacja** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **UTM** | | |
|  | **Wymagania Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * firewall, * ochrony w warstwie aplikacji, * protokołów routingu dynamicznego. |
|  | **Redundancja, monitoring i wykrywanie awarii** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN.  System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
|  | **Interfejsy, Dysk, Zasilanie** | System realizujący funkcję Firewall musi dysponować minimum:   * 10 portami Gigabit Ethernet RJ-45, * 8 gniazdami SFP 1 Gbps, * 2 gniazdami SFP+ 10 Gbps.   System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.  System musi być wyposażony w zasilanie AC. |
|  | **Parametry wydajnościowe** | W zakresie Firewall’a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.  Przepustowość Stateful Firewall: min. 36 Gbps.  Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: min. 14 Gbps.  Wydajność szyfrowania IPSec VPN: min. 18 Gbps.  Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix – min. 5.2 Gbps.  Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 4.7 Gbps.  Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – min. 5.7 Gbps. |
|  | **Funkcje Systemu Bezpieczeństwa** | Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  Kontrola Aplikacji.  Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.  Ochrona przed atakami - Intrusion Prevention System.  Kontrola stron WWW.  Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  Zarządzanie pasmem (QoS, Traffic shaping).  Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).  Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  Analiza ruchu szyfrowanego protokołem SSL.  Analiza ruchu szyfrowanego protokołem SSH. |
|  | **Polityki, Firewall** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * translację jeden do jeden oraz jeden do wielu, * dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
|  | **Połączenia VPN** | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:   * wsparcie dla IKE v1 oraz v2, * obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), * obsługa protokołu Diffie-Hellman grup 19 i 20, * wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, * tworzenie połączeń typu Site-to-Site oraz Client-to-Site, * monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, * możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, * obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth, * mechanizm „Split tunneling” dla połączeń Client-to-Site.   System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:   * pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0, * pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
|  | **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego, * Policy Based Routingu, * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.   System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
|  | **Zarządzanie pasmem** | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
|  | **Kontrola Antywirusowa** | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.  System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. |
|  | **Ochrona przed atakami** | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.  Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.  System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.  Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
|  | **Kontrola aplikacji** | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
|  | **Kontrola WWW** | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.  Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
|  | **Uwierzytelnianie użytkowników w ramach sesji** | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:   * haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, * haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, * haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.   Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.  Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
|  | **Zarządzanie** | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.  Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.  Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.  System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
|  | **Logowanie** | W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  Musi istnieć możliwość logowania do serwera SYSLOG. |
|  | **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall, * ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW, * ICSA dla funkcji SSL VPN. |
|  | **Licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |
|  | **Gwarancja** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Komputer stacjonarny** | | |
|  | Typ | Komputer stacjonarny All in One. |
|  | Procesor | Min. 6 rdzeniowy min. 6 wątkowy, taktowanie min. 3.1GHz, w trybie turbo min. 4.6GHz, min. 9MB pamięci podręcznej, zużycie energii max. 65W.  Procesor powinien osiągać min. 13 430 pkt. w teście PassMark na dzień składania ofert. Wyniki testów dostępne są na stronie: https://www.cpubenchmark.net/cpu\_list.php |
|  | Pamięć RAM | min. 8GB DDR4 min. 2666 MHz. |
|  | Dysk twardy | Dysk twardy SSD M.2 NVMe, min. 256GB. |
|  | Karta graficzna | Zintegrowana. |
|  | Ekran | min. 23,8” IPS WLED min. 1920 x 1080 pikseli. |
|  | Karta sieciowa | Wbudowana karta sieciowa Ethernet min. 10/100/1000 GBps.  Wbudowana karta sieciowa bezprzewodowa WiFi min. 802.11ac +. Bluetooth min. 4.2. |
|  | Interfejsy | Z boku obudowy:   * min. 1x USB 3.1 Typ C Gen 2, * min. 1x USB 3.1 Typ A Gen 1 PowerShare, * min. 1x Czytnik kart pamięci, * min. 1x Uniwersalne złącze Jack.   Z tyłu obudowy:   * min. 2x USB 3.1 Typ A Gen 1, * min. 2x USB 3.1 Typ A Gen 2, * min. 1x DisplayPort, * min. 1x HDMI In, * min. 1x HDMI Out, * min. 1x Audio Line-Out, * min. 1x RJ-45, * min. Gniazdo zasilania. |
|  | Multimedia | Wbudowana kamera min. 2.0 MPx, z opcją wysuwania, podczerwieni i rozdzielczości Full HD można ukryć, gdy nie jest używana. Ponadto kamera zapewnia dodatkową ochronę dzięki funkcji rozpoznawania twarzy Windows Hello. |
|  | Napęd DVD | Wbudowany napęd DVD+/-RW. |
|  | Podstawa monitora | Z regulowaną wysokością.  Demontaż standu musi odbywać się bez użycia narzędzi, mocowanie standu opatrzone w przycisk zwalniający. Demontaż tylnej pokrywy musi odbywać się również bez użycia narzędzi, nie dopuszcza się stosowania śrub motylkowych, radełkowych czy zwykłych wkrętów. |
|  | Zasilacz | Wbudowany zasilacz min. 155W z certyfikatem 80PLUS BRONZE lub równoważnym. |
|  | Gwarancja | min. 36 miesiące na miejscu u klienta następnego dnia roboczego. |
|  | System operacyjny | **Zainstalowany system operacyjny Microsoft Windows 10 Professional 64bit PL lub równoważny.**  Po przez równoważność zamawiający rozumie:   * licencja na zaoferowany system operacyjny musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania, * interfejsy użytkownika dostępne w kilku językach do wyboru – minimum w polskim i angielskim, * funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika, * 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 – wymagane podanie nazwy strony serwera www, * możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, * dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, * wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6, * wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, * zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe, * graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, * wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), * funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, * możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę Zamawiający rozumie zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, * rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, * możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, * zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników, * 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, * zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi, * możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących), * wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny, * mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), * wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), * wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, * wsparcie dla algorytmów Suite B (RFC 4869), * wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, * wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk, * wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, * wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, * zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, * 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, * transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, * zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe, * udostępnianie modemu, * oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, * możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, * 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.), * możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu), * Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych, * mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z  możliwością szyfrowania ograniczonego do danych użytkownika, * Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych, * Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych, * możliwość nieodpłatnego instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu, * zaoferowane oprogramowanie musi pozwalać na przenoszenie pojedynczych sztuk oprogramowania do jednostek zależnych. |
| **Laptop** | | |
|  | Typ | Komputer przenośny |
|  | Procesor | Min. 4 rdzenie, taktowanie min. 1.6 GHz w trybie turbo min. 4.2 GHz, min. 6MB pamięci podręcznej.  Procesor powinien osiągać min. 8 550 pkt. w teście PassMark na dzień składania oferty. Wyniki testów dostępne są pod adresem: https://www.cpubenchmark.net/cpu\_list.php |
|  | Pamięć RAM | min. 8GB RAM DDR4. |
|  | Dysk SSD | min. 256GB M.2 NVMe.  Możliwość zamontowania drugiego dysku SATA, elementy montażowe powinny znajdować się w laptopie. |
|  | Karta graficzna | Zintegrowana. |
|  | Ekran | Min. 15,6” Matowy LED, min. 1920 x 1080 pikseli. |
|  | Napęd DVD | Wbudowany napęd DVD+/-RW. |
|  | Kamera internetowa | min. 1.0 Mpix. |
|  | Dźwięk | Zintegrowana karta dźwiękowa.  Wbudowane głośniki stereo.  Wbudowany mikrofon. |
|  | Sieć | Karta Ethernet min. 10/100/1000.  WiFi min. 802.11 a/b/g/n/ac.  Bluetooth. |
|  | Złącza | Min. 2x USB 3.1 gen. 1  Min. 1x HDMI  Min. 1x Czytnik kart SD  Min. 1x USB 2.0  Min. 1x VGA  Min. 1x RJ-45  Min. 1x Złącze jack combo |
|  | Bateria | Min. 3 komorowa, min. 3500 mAh |
|  | Waga | Max. 2.1 kg |
|  | Wymiary (wys. x szer. x gł.) | Max. 23,6 x 38 x 25,8 mm |
|  | Dodatkowe informacje | Wydzielona klawiatura numeryczna.  Możliwość zabezpieczenia linką.  Wbudowany czytnik linii papilarnych.  Szyfrowanie TPM. |
|  | Kolor | Czarny lub równoważny. |
|  | Wyposażenie dodatkowe | Torba transportowa do laptopa, pasująca wymiarami do laptopów o przekątnej 15,6”. Oddzielna komora na laptopa, dokumenty i akcesoria. Pasek na ramię. Torba powinna być usztywniona, aby zapobiegać ew. uszkodzeniom urządzenia.  Mysz bezprzewodowa optyczna lub laserowa, min. 2 klawisze, rolka. Wyposażona w nano odbiornik. Do zestawu dołączone baterie odpowiednie do zasilanie myszki. |
|  | Gwarancja | Min. 36 miesięcy, naprawa powinna odbywać się na miejscu u zamawiającego, na następny dzień roboczy. |
|  | System operacyjny | **Zainstalowany system operacyjny Microsoft Windows 10 Professional 64bit PL lub równoważny.**  Po przez równoważność zamawiający rozumie:  1. Licencja na zaoferowany system operacyjny musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania.  2. Interfejsy użytkownika dostępne w kilku językach do wyboru – minimum w polskim i angielskim.  3. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.  4. 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 – wymagane podanie nazwy strony serwera www.  5. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  6. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  7. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  8. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  9. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.  10. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.  11. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).  12. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.  13. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę Zamawiający rozumie zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.  14. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.  15. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.  16. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  17. 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.  18. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.  19. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  20. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny  21. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  22. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.  23. Wsparcie dla algorytmów Suite B (RFC 4869).  24. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.  25. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.  26. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  27. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.  28. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  29. 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.  30. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  31. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.  32. Udostępnianie modemu.  33. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  34. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  35. 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.).  36. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).  37. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.  38. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.  39. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.  40. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.  41. Możliwość nieodpłatnego instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.  42. Zaoferowane oprogramowanie musi pozwalać na przenoszenie pojedynczych sztuk oprogramowania do jednostek zależnych. |
| **Tablet** | | |
|  | Wyświetlacz | Wyświetlacz Multi-Touch o przekątnej min. 9,7 cala z podświet­leniem LED, w technologii IPS.  Rozdzielczość min. 2048 na 1536 pikseli przy min. 264 ppi.  Powłoka oleofobowa odporna na odciski palców. |
|  | Wielkość pamięci | Min. 32 GB |
|  | Procesor | min. 4 rdzeniowy, o taktowaniu min. 1.64 GHz do min. 2.34 GHz |
|  | Złącze | Min. 1x Lighting |
|  | Aparat | Aparat min. 8-megapikse­lowy  Live Photos  Autofokus  Panorama (do min. 43 megapikseli)  Tryb HDR dla zdjęć  Kontrola ekspozycji  Tryb zdjęć seryjnych  Ustawianie ostrości stuknięciem  Tryb samowyzwalacza  Światło przysłony min. ƒ/2,4  Pięcio­elementowy obiektyw  Hybrydowy filtr IR  Matryca BSI  Automatyczna stabilizacja obrazu  Dodawanie geoznaczników do zdjęć |
|  | Nagranie wideo | Nagrywanie wideo min. HD 1080p  Wideo w zwolnionym tempie (min. 120 kl./s)  Wideo poklatkowe ze stabilizacją obrazu  Stabilizacja obrazu wideo  min. 3-krotne powiększenie wideo  Dodawanie geoznaczników do wideo |
|  | Sieć | Wi‑Fi (802.11a/b/g/n/ac); dwa zakresy (2,4 GHz i 5 GHz); HT80 z technologią MIMO  Technologia Bluetooth min. 4.2 |
|  | Czujniki | Żyroskop trójosiowy  Przyspieszen­io­mierz  Barometr  Czujnik oświetlenia zewnętrznego  Czytnik linii papilarnych w przycisku |
|  | Zasilanie i bateria | Wbudowana bateria litowo-polimerowa o pojemności min. 32,4 Wh (do wielokrotnego ładowania)  min. 10 godzin czas pracy na baterii  Ładowanie przez zasilacz lub przewód USB podłączony do komputera |
|  | Wymiary (Wys. x Szer. x Gł.) | Max. 240 cm / max. 170 cm / max. 8 mm |
|  | Waga | Max. 470g |
|  | Zawartość opakowania | Tablet  Przewód z Lightning na USB  Zasilacz USB |
|  | Kolor | Szary lub równoważny |
|  | Gwarancja | min. 24 miesięcy |
|  | Dodatkowa ochrona | **Szkło hartowane na ekran –** powinna się charakteryzować zwiększoną odpornością na pękanie, posiadająca twardość min. 9H, wysokość szkła nie może przekraczać 0,3 mm.  **Etui na tablet –** etui wykonane z wytrzymałego poliwęglanu oraz trwałego tworzywa TPU. Etui powinno posiadać technologię, która amortyzuje urządzenie i absorbuje wstrząsy podczas upadku. Idealnie dopasowane, w pełni funkcjonalne, nie ograniczające dostępu do portów zewnętrznych i skutecznie chroniące przed zarysowaniami. Etui powinno posiadać certyfikat MIL STD 810G-516.6 lub równoważny. |
| **Zasilacz awaryjny UPS** | | |
|  | Typ | Zasilacz awaryjny |
|  | Moc pozorna | 5000 VA |
|  | Moc rzeczywista | 4500 W |
|  | Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line |
|  | Typ obudowy | Uniwersalna tower/rack |
|  | Sprawność UPS'a | > 93% w trybie podwójnego przetwarzania on-line przy 100% obciążeniu |
|  | Liczba, typ gniazd wyjściowych | Podłączenie na stałe - listwa zaciskowa oraz min. 8 x IEC 320 C13 (10A) i min. 2 x IEC 320 C19 (16A) - wszystkie wyjścia z podtrzymaniem zasilania i ochroną przepięciową. Gniazda odbiorcze podzielone muszą być na co najmniej dwa segmenty, których sterowanie odbywać się powinno za pomocą dołączonego oprogramowania. |
|  | Urządzenie winno posiadać | Dwutorowe zasilanie wejścia: oddzielne wejście zasilania prostownika i bypassu wewnętrznego |
|  | Typ gniazda wejściowego | Zaciski |
|  | Wymagany czas podtrzymania dla obciążenia mocą 3500W min. | 5 minut |
|  | Dodatkowe baterie | Możliwość wydłużenia czasu podtrzymania do > 1,5h przy obc. mocą 3500W poprzez dołożenie dodatkowych modułów baterii zewnętrznych. |
|  | Napięcie znamionowe | 230V |
|  | Tolerancja napięcia prostownika | 100-276V przy 40% obciążeniu |
|  | Częstotliwość znamionowa | 50/60 Hz autodetekcja |
|  | Tolerancja częstotliwości | 40 – 70 Hz |
|  | Kształt napięcia | Sinusoidalny |
|  | Napięcie znamionowe wyjściowe | 230 V (domyślnie) / 200/208/220/240V |
|  | Zakres zmian napięcia wyjściowego | +/-1% napięcia nominalnego |
|  | Częstotliwość wyjściowa | 50/60 Hz +/-0,5% |
|  | Całkowite odkształcenia napięcia THDu | < 2% dla obciążenia liniowego |
|  | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
|  | Ochrona przed przeładowaniem | Tak |
|  | Ochrona przed głębokim rozładowaniem | Tak |
|  | Okresowy automatyczny test baterii | Tak |
|  | Zimny start | Tak |
|  | System zarządzania pracą baterii | System nieciągłego ładowania baterii.  Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. |
|  | Interfejs komunikacyjny | • USB |
|  |  | • RS232 DB-9 żeński (HID) |
|  |  | • miniport wyłącznik awaryjny RPO |
|  |  | • miniport wyłącznik ON/OFF |
|  |  | • DB-9 port przekaźnikowy |
|  |  | • DB15 interfejs do komunikacji równoległej |
|  | Panel sterowania z wyświetlaczem LCD | • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS’a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh).   • Przyciski sterowania.   • Wskaźniki stanu: trybu online, trybu bateryjnego, trybu bypass, usterki. |
|  | Przyciski sterujące i wskaźniki diodowe LED | • sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie)   • przycisk Escape (anulowanie)   • przyciski funkcyjne (przewijanie w górę i w dół)   • przycisk Enter (potwierdzający)  • przycisk ON/OFF załączenia i wyłączenia |
|  | Wyposażenie standardowe | •  kabel RS232   • 2 kable IEC   •  kabel USB   •  oprogramowanie na CD   •  uchwyty kablowe   •  podstawki do montażu pionowego (wieża)   •  zestaw szyn montażowych do szafy 19"   •  instrukcja obsługi |
|  | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii (minimum: Windows: 2000, XP, 2003, Vista, Server 2008, 7; Linux: Red Hat, Fedora Core, SuSE, VMware ESX; UNIX: AIX, HP-UX, SCO, SGI Irix, Mac OS, Sun Solaris; Novell NetWare do v 6.5). Oprogramowanie musi pozwalać na integrację z platformą wirtualizacyjną Vmware: vCenter Server. Oprogramowanie musi mieć możliwość wyboru polskiej wersji językowej. |
|  | Maksymalna wysokość | 3U |
|  | Maksymalna głębokość | 690 mm |
|  | Poziom hałasu w odl. 1m | ≤ 45 dBA |
|  | Zgodność z normami UE | Deklaracja producenta o zgodności z wymaganymi dla tego typu urządzeń normami UE |
|  | Dodatkowe certyfikaty | ISO 9001 dla producenta urządzenia lub równoważne |
|  | Gwarancja | 3 lata |
| **System kopii zapasowej** | | |
|  | **Licencje** | Licencja wieczysta, typu per 1CPU w ilości umożliwiającej zalicencjonowanie 4 hostów fizycznych po 1 CPU każdy. |
|  | **Wymagania ogólne** | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. 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. |
|  | **Koszty posiadania** | 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 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 zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować również 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 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. |
|  | **Wymagania RPO** | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.  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 plików na taśmy.  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 wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 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). |
|  | **Wymagania RTO** | 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, Microsoft Azure Stack oraz Amazon EC2.  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 obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.  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.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.  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 |
|  | **Inne** | Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
|  | **Serwis** | 3 lata, z czasem wsparcia co najmniej 12x5, tj. przez 12 godz. 5 dni roboczych na każdy element oprogramowania |
| **System wirtualizacji serwerów** | | |
|  | **Licencje** | Należy dostarczyć licencję oprogramowania (w ilości zgodnej z zamawianymi procesorami) wraz z systemem do zarządzania infrastrukturą wirtualną |
|  | **Funkcjonalność** | * Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. * Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. * Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. * Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12 TB pamięci fizycznej RAM. * Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. * Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. * Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM. * Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. * Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. * Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. * Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. * Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. * Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. * Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej. * Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. * Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. * Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. * Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. * Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny. * Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych. * Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. * Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. * Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie. * Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. * Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory. * System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów; * Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.   Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN); |
|  | **Serwis** | 3 lata na każdy element oprogramowania wirtualizacyjnego |
| **Licencje systemów operacyjnych** | | |
|  | **Opis** | 4 szt. licencji serwerowego systemu operacyjnego zgodnego z Microsoft Windows Server w najnowszej dostępnej na rynku wersji – zgodnie z warunkami licencjonowania do zalicencjonowania 10 szt. maszyn wirtualnych z systemami Microsoft Windows Server 2019, 2016 i 2012R2 zmigrowanych z innych środowisk na klaster wirtualizacyjny utworzony z oferowanych serwerów wirtualizacji. Licencja na oprogramowanie musi pozwalać na zainstalowanie systemu na serwerze z 1 lub 2 fizycznymi procesorami z sumaryczną ilością rdzeni jak w oferowanych serwerach wirtualizacyjnych. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i na 2 maszynach wirtualnych. Licencja musi uprawniać do instalacji starszych wersji oferowanego Serwerowego systemu operacyjnego. |
| **Oprogramowanie bazodanowe** | | |
|  | **Opis ogólny** | 4 licencje (lub zgodnie z licencjonowaniem producenta bazy danych dla 2 serwerów) na motor bazy danych typu Oracle Standard Edition Two lub kompatybilny umożliwiająca uruchomienie na 2 fizycznych procesorów klasy intel x86 (po 1 w 2 serwerach spiętych w klaster – serwer wirtualny). Licencja musi być dożywotnia, bez ograniczeń formalnych na wykorzystanie z aplikacjami pochodzącymi od dowolnych dostawców. Wraz z licencją należy dostarczyć usługę gwarancji producenta na okres **minimum 36 miesięcy.** |
|  | **Wsparcie** | Oprogramowanie musi wspierać posiadany przez Zamawiającego system HIS CliniNet, ver. 7.73.1 (2019.MS.3.13) producenta CompuGroup Medical Polska Sp. z o.o. |
|  | **Opis szczegółowy** | Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla Itanium, Solaris dla procesorów SPARC/x86-64, IBM AIX), Intel Linux 64-bit, MS Windows 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach.  Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych.  Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego.  Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji powinien pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, z kolei spójny odczyt nie powinien blokować możliwości wykonywania zmian.  Oznacza to, że modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia,  niezależnie od modyfikacji przeglądanego zbioru danych.  Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).  Możliwość migracji 8-bitowego zestawu znaków bazy danych (np. MS Windows CP 1252, ISO 8859-2) do Unicode.  Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych.  Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).  Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu.  Możliwość kompilacji procedur składowanych w bazie danych do postaci kodu binarnego.  Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).  W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek.  Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.  Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.  Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, Data Protector itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online.  Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup).  Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.  W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników.  Wsparcie dla typu danych DICOM obsługiwanego wewnętrznie przez serwer bazy danych.  Możliwość zakładania w tabelach kolumn typu obsługującego standard DICOM.  Możliwość przeszukiwania zakładania indeksów na grupie atrybutów metadanych składowanych w kolumnach przechowujących dane w formacie DICOM.  Możliwość przeszukiwania metadanych:   * wszystkich bądź niektórych atrybutów, * możliwość zakładania indeksów na wybranych atrybutach, * możliwość wyszukiwania pełno tekstowego, * możliwość nawigacji zgodnej z hierarchią atrybutów.   Składowanie metadanych DICOM i treści DICOM odbywa się wewnątrz bazy danych.  Operowanie na danych DICOM za pomocą konstrukcji języka SQL, procedur składowanych, dostęp za pomocą Java API.  Wbudowane mechanizmy konwersji treści DICOM do formatów JPEG, GIF, MPEG, AVI.  Możliwość budowy klasta typu active-active opartego o minimalnie 2 węzły (maksymalnie 2 x 1 CPU)  Możliwość zwiększenia przepustowości bazy danych poprzez uruchomienie dodatkowych serwerów obsługujących tą samą bazę danych (w klastrze).  Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej (zmiana organizacji plików danych) oraz logicznej struktury baz danych (tabel / indeksów).  Unieruchomienie jednego z serwerów bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów  Możliwość kontynuacji pracy użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Powinna istnieć możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia.Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera do którego zostało nawiązane połączenie |

\* **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.