Załącznik nr 1 do OPZ

na dostawę i instalację infrastruktury teleinformatycznej

**Specyfikacja przedmiotu zamówienia**

**sprzęt serwerowo-sieciowy**

**Zamawiający - Partner nr 43**

**Ośrodek Badawczo-Naukowo-Dydaktyczny Chorób Otępiennych im. Księdza Henryka Kardynała Gulbinowicza – Ośrodek Alzheimerowski w Ścinawie**

w projekcie ,,Wprowadzenie nowoczesnych e-Usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia”

**MIEJSCE DOSTAWY:**

ul. Jana Pawła II nr 12

59-330 Ścinawa

# 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** | **Podstawowy zakres zakupów:**  **Liczba zamawianego sprzętu (sztuk)** | **Zakupy objęte prawem opcji:**  **Liczba zamawianego sprzętu (sztuk)** | **Zakupy łączne** |
|  | **Serwer1** | 2 | Zamawiający nie przewiduje prawa opcji | 2 |
|  | **Serwer2** | 3 | 3 |
|  | **Pamięć masowa NAS** | 2 | 2 |
|  | **UPS serwerowy** | 5 | 5 |
|  | **Przełącznik dystrybucyjny 48p** | 6 | 6 |
|  | Moduł SFP+ | 14 | 14 |
|  | **Punkt dostępowy** | 39 | 39 |
|  | **UTM** | 1 | 1 |
|  | **Oprogramowanie backupowe do serwerów** | 5 | 5 |
|  | **Oprogramowanie do zarządzania infrastrukturą IT** | 1 | 1 |
|  | **System operacyjny komplet licencji dla zaoferowanego serwera** | 7 |  | 7 |
|  | Licencje dostępowe | 40 |  | 40 |
|  | Licencje dostępowe zdalne | 40 |  | 40 |
|  | **Szafa serwerowa typu RACK 42U** | 1 |  | 1 |

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

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

# Serwer#1

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Serwer#1** | | |
| 1. | **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 4 dysków 3.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack. |
| 2. | **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. |
| 4. | **Procesor** | Zainstalowany jeden procesor ośmio-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 65 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| 5. | **RAM** | 32GB RDIMM 2666MHz, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| 6. | **Zabezpieczenia pamięci RAM** | Advanced ECC lub równoważny |
| 7. | **Gniazda PCI** | min. 2 sloty Gen. 3. |
| 8. | **Interfejsy sieciowe/FC** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T.  Zainstalowana jedna karta dwuportowa 10GbE BaseT. |
| 9. | **Napęd optyczny** | Brak |
| 10. | **Dyski twarde** | Zainstalowane 4 x 480GB SSD SATA Mix Use 6 Gbps  Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash o pojemności minimum 32GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| 11. | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| 12. | **Wbudowane porty** | min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| 13. | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| 14. | **Wentylatory** | Redundantne |
| 15. | **Zasilacze** | Redundantne, Hot-Plug maksymalnie 550W. |
| 16. | **Bezpieczeństwo** | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  TPM 2.0 |
| 17. | **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 * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) * szyfrowane połączenie (SSLv3) 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, Telnet, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * wsparcie dla dynamic DNS * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232   możliwość zarządzania bezpośredniego oraz poprzez złącze USB umieszczone na froncie obudowy. |
| 18. | **Certyfikaty** | Serwer musi posiadać deklaracja CE. |
|  | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2016, 2019  Red Hat Enterprise Linux (RHEL) 6.9 oraz 7.3  SUSE Linux Enterprise Server (SLES) 11 SP4 oraz 12 SP2  VMware ESXi 6.0, 6.5 i 6.7 |
| 19. | **Warunki gwarancji** | 3 lata gwarancji producenta z czasem naprawydo 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. |
| 20. | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# Serwer#2

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Serwer#2** | | |
| 1. | **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 4 dysków 3.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack. |
| 2. | **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
|  |  |  |
| 4. | **Procesor** | Zainstalowany jeden procesor ośmio-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 65 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| 5. | **RAM** | 32GB RDIMM 2666Hz, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| 6. | **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror |
| 7. | **Gniazda PCI** | min. 2 sloty Gen. 3. |
| 8. | **Interfejsy sieciowe/FC** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T.  Zainstalowana jedna karta dwuportowa 10GbE BaseT. |
| 9. | **Napęd optyczny** | Brak |
| 10. | **Dyski twarde** | Zainstalowane 4 x 480GB SSD SATA Mix Use 6 Gbps  Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash o pojemności minimum 32GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| 11. | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| 12. | **Wbudowane porty** | min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| 13. | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| 14. | **Wentylatory** | Redundantne |
| 15. | **Zasilacze** | Redundantne, Hot-Plug maksymalnie 550W. |
| 16. | **Bezpieczeństwo** | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  TPM 2.0 |
| 17. | **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 * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) * szyfrowane połączenie (SSLv3) 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, Telnet, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * wsparcie dla dynamic DNS * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232   możliwość zarządzania bezpośredniego oraz poprzez złącze USB umieszczone na froncie obudowy. |
|  |  |  |
|  | Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2016, 2019  Red Hat Enterprise Linux (RHEL) 6.9 oraz 7.3  SUSE Linux Enterprise Server (SLES) 11 SP4 oraz 12 SP2  VMware ESXi 6.0, 6.5 i 6.7 |
| 19. | **Warunki gwarancji** | 3 lata gwarancji producenta z czasem naprawydo 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. |
| 20. | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# Pamięć masowa NAS

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Pamięć masowa NAS** | | |
| 1. | **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji min.12 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack.  Pamięć masowa musi mieć możliwość rozbudowy. |
| 2. | **Procesor** | min. cztero-rdzeniowy, klasy x86 |
| 3. | **RAM** | min. 4 GB Pamięci RAM |
| 4. | **Porty** | Min. 3x USB 3.1, 4x RJ-45 1GbE,2x 10GbE SFP+  Min. 2x nieobsadzone porty PCIe Gen3 |
| 5. | **Zainstalowane Dyski** | Min. 12x 8TB 3,5” 7200rpm 6Gb/s SATA 128MB cache – dedykowane do NAS-a |
| 6. | **Obsługiwane Systemy plików** | EXT4,EXT3,NTFS |
| 7. | **Obsługiwane poziomy RAID** | * RAID 0 * RAID 1 * RAID 5 * RAID 6   RAID 10 |
| 8. | **Zasilacze** | Redundantne, Hot-Plug |
| 9. | **Warunki gwarancji** | 36 miesięcy gwarancji  W przypadku awarii dysków pozostają one własnością Zamawiającego. |

# UPS serwerowy

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | |
| --- | --- | --- | --- |
| **UPS serwerowy** | | | |
|  | Moc pozorna | min. 3000VA | |
|  | Moc rzeczywista | min. 3000W | |
|  | Technologia | on-line (VFI), podwójna konwersja | |
|  | Sprawność max (dla VFI) | ˃ 90 % | |
|  | Praca sieciowa | Napięcie wejściowe | 110 ÷ 300 V AC ± 5% |
| Kształt napięcia wyjściowego | sinusoidalny |
| Czas przełączania sieć – UPS | 0ms |
| Współczynnik odkształceń prądu wejściowego THDi | < 10% |
|  | Praca bateryjna | Napięcie wyjściowe | ~230V |
| Kształt napięcia wyjściowego na pracy bateryjnej | sinusoidalny |
| Zabezpieczenie przeciwzwarciowe gniazd wyjściowych | Bezpiecznik automatyczny 16 A |
| Zabezpieczenie przeciążeniowe | elektroniczne |
| Akumulatory wewnętrzne w UPS / w Module Bateryjnym | minimum 12V 9Ah; szczelne, bezobsługowe |
| Czas podtrzymania (100 % Pmax) | minimum 3 minuty |
| Czas ładowania baterii wew w UPS i w modułach bateryjnych (nie zależnie od ilości podłączonych modułów) - po 80% wyładowaniu baterii | do 3h |
|  | Pozostałe | Przeciążalność | 110 % ÷ 120 % = 60s, >120 % = 100ms |
| Wejście zasilania | 1 x IEC 320 C20 (16 A) |
| Ilość i typ gniazd wyjściowych | min 8x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16 A), z czego minimum 4 gniazda sterowalne |
| Sygnalizacja | Wyświetlacz LCD |
| Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych | Wymagana możliwość podłączenia do 10 zewnętrznych modułów bateryjnych |
| Interfejs komunikacyjny | RS232, USB HID, SNMP |
| Remote ON/OFF – możliwość zdalnego załączenia/wyłączenia zasilacza | wymagane |
| Złącze EPO | wymagane ustawienie NC |
| Gwarancja | minimum 36 miesięcy na elektronikę i 36 miesięcy na akumulatory; |
| Obudowa | Rack 19” wraz z szynami montażowymi |
| Serwis | * autoryzowany serwis producenta zlokalizowany w Polsce. * naprawa w maksymalnie 5 dni roboczych   serwis realizowany w systemie door to door |
| Oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer |
| Certyfikaty producenta | deklaracja CE |
| Oświadczenia / dokumenty | jeżeli oferowana jest rozszerzona gwarancja producenta to wymagane jest dołączenie dokumentu potwierdzającego realizację gwarancji przez serwis producenta (zapis w karcie gwarancyjnej lub oświadczenie producenta) |

# Przełącznik dystrybucyjny

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Przełącznik dystrybucyjny** | | |
|  | **Obudowa** | Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19” |
|  | **Pamięć** | Minimum RAM: 512MB  Minimum FLASH : 32MB |
|  | **Interfejsy 1Gb** | Minimum 48 gigabitowe interfejsy PoE RJ-45 100/1000 Mbps,  4 interfejsy 10 Gigabit SFP+ |
|  | **Wydajność** | * Potencjał przełączania nie mniejszy niż 176 Gbps * Prędkość przełączania/Przepustowość nie mniejsza niż  130,9 Mbps * Bufor pakietu nie mniejszy niż 1500 KB * Tabela adresów MAC nie mniejsza niż 16K   Minimalny budżet PoE – 375W |
|  | **Tryby pracy** | Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia |
|  | **Zgodność ze standardami** | * IEEE 802.3 10BASE-T Ethernet * IEEE 802.3u 100BASE-TX Ethernet\* * IEEE 802.3ab 1000BASE-T Ethernet\* * IEEE 802.3z 1000BASE-X\* * IEEE 802.3ae 10-Gigabit Ethernet Over Fiber\* * IEEE 802.3af PoE\* * IEEE 802.3at PoE Plus\* * IEEE 802.3az EEE\* * IEEE 802.3x flow control * IEEE 802.3ad LACP aggregation\* * IEEE 802.1D Spanning Tree Protocol (STP) * IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) * IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) * IEEE 802.1p Class of Service (CoS) prioritization * IEEE 802.1X port authentication |
|  | **Odporność i dostępność** | * IEEE 802.1D Spanning Tree Protocol (STP) * IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) * IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) * IEEE 802.3ad LACP (Max # Trunks/ Links per Trunk): 8/8 * Loop guard * ErrDisable recovery * Dual configuration files * Dual images |
|  | **Kontrola ruchu** | * 802.1Q Static VLANs/Dynamic VLANs: 1K/4K * Support up to 4K VLAN ID * Independent VLAN Learning (IVL) * L2PT * Port-based VLAN * Voice VLAN * VLAN trunking * GVRP |
|  | **Bezpieczeństwo** | * 802.1X * Port security * MAC authentication * Static MAC forwarding * SSL * Static ARP * Policy-based security filtering * Port isolation * MAC search * Guest VLAN * PPPoE relay agent * PPPoE option 82 * PPPoE IA * Interface related trap enable/ disable (by port) * CPU protection * SHA2 HTTPS certification * Login authentication by RADIUS * RADIUS accounting * Authorization on RADIUS * Multiple RADIUS servers * 802.1x VLAN and bandwidth assignment by RADIUS * ACL packet filtering (IPv4/IPv6) |
|  | **QoS** | * No. of hardware queues per port: 8 * 802.1p queuing methods: SPQ, WRR, WFQ * Storm control: broadcast, unknown L2MC, unknown unicast (DLF) * Rate limiting per port * Policy-based rate limiting * Policy-based prioritization |
|  | **Layer 2 Multicast** | * L2 multicast group: 1K * IGMP snooping (v1, v2, v3) * Configurable IGMP snooping timer and priority * IGMP snooping statistics * IGMP throttling * IGMP filtering * Static multicast |
|  | **Layer 3 Routing** | * Static route * Assigned DHCP relay with specific source IP interface |
|  | **Zarządzanie** | * SNMP v1, v2c, v3 * SNMP trap group * RMON (1, 2, 3, 9) * Syslog (IPv4/v6) * IEEE 802.1AB LLDP * IEEE 802.1AB LLDP-MED * Custom default * Display port utilization |
|  | **Zarządzanie IPv6** | * IPv6 over Ethernet (RFC 2464) * IPv6 addressing architecture (RFC 4291) * Dual stack (RFC 4213) * ICMPv6 (RFC4884) * Path MTU (RFC 1981) * Minimum path MTU size of 1280 (RFC 5095) * Encapsulation for maximum MTU of 1500 * Neighbor discovery (RFC 4861) * DHCPv6 relay * Default DHCP client mode * Duplicated Address Detection (DAD) |
|  | **Zarządzanie urządzeniem** | * Standalone management by Web interface * Cloud management * Setup Wizard * Management through Telnet * Management through Web, SNMP * Firmware upgrade by FTP/Web * Configuration saving and retrieving * Multiple login supported * Configure clone * DHCP relay per VLAN * DHCP client IPv4 * DHCP client IPv6 * DHCP option 82 * Daylight saving * NTP Server (IPv4/IPv6) – Support DNS format * Port mirroring * Scheduled PoE * PoE default consumption mode * PoE power management extended configuration * Web login warning page * Restore to last custom default |
|  | **MIB** | * RFC 1066 TCP/IP-based MIB * RFC 1213, 1157 SNMPv2c/v3 MIB * RFC 1493 bridge MIB * RFC 1643 Ethernet MIB * RFC 1757 RMON Group 1, 2, 3, 9 * RFC 2011, 2012, 2013 SNMPv2 MIB * RFC 2233 SMIv2 MIB * RFC 2358 Ethernet-like MIB * RFC 2674 bridge MIB extension * RFC 2819, 2925 remote management MIB * RFC 3621 power Ethernet MIB * RFC 4022 management information base for transmission control protocol * RFC 4113 management information base for user datagram protocol * RFC 4292 IP forwarding table MIB * RFC 4293 Management Information Base (MIB) for IP |
|  | **Zakres temperaturowy pracy** | 0°C - 50°C |
|  | **MTBF (hr)** | Parametr te nie powinien być niższy niż 494,960 |
|  | **Gwarancja** | Urządzenie powinno posiadać ograniczoną dożywotnią gwarancję producenta |
|  | **Serwis** | W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat. |
|  | **Wymagane Certyfikaty** | Bezpieczeństwo  • LVD  • BSMI  EMC  • FCC Part 15 (Class A)  • CE EMC (Class A)  • BSMI EMC  RoHS  • Level A |
|  | **Pozostałe** | Sprzęt musi być fabrycznie nowy i pochodzić z polskiego kanału dystrybucji |
|  |  | Moduł SFP+ |
|  | Wymaganie ogólne | Wykonawca dostarczy 14 sztuk modułów SFP+ zalecanych przez producenta przełącznika. |

# Punkt dostępowy

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa parametru** | **Wymagane parametry** |
| 1 | Obudowa | Obudowa urządzenia musi być przystosowana do montażu do sufitowego lub ściennego. |
| 2 | Ilość portów | Urządzenie w standardzie musi posiadać 2 gigabitowe porty LAN (10/100/1000 Mbps) |
| 3 | Tryb pracy | Urządzenie musi umożliwiać pracę w jednym z poniższych trybów:   * samodzielny (standalone) * zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia * zarzadzanie poprzez kontroler sprzętowy |
| 4 | Funkcje WLAN | Urządzenie musi:   * posiadać co najmniej dwa radia * obsługiwać technologię 2x2 MIMO dla częstotliwości 2,4GHz i 3x3 MIMO dla częstotliwości 5GHz * jednocześnie obsługiwać dwa zakresy częstotliwości 2.4 GHz i 5 GHz (SU-MIMO i MU-MIMO) * wspierać standard 802.11ac Wave 2 * wspierać Band Steering * wspierać WDS/Mesh * wspierać DCS i Load Ballancing * wspierać Fast Roaming (Pre-authentication, PMK caching and 802.11 r/k/v) |
| 5 | Bezpieczeństwo | Urządzenie musi: wspierać:   * WEP * WPA/WPA2-PSK * WPA/WPA2-Enterprise * EAP (-TLS, -TTLS, -PEAP, -FAST, -AKA and -SIM) * IEEE 802.1X * MAC filtering * L2 isolation * RADIUS authentication * Rogue AP detection |
| 6 | Funkcje sieci | Urządzenie musi: wspierać:   * IPv6 host * VLAN * WMM * U-APSD * DiffServ marking |
| 7 | Zarzdądzanie | Urządzenie musi: wspierać zarzadzanie poprzez:   * Web UI * CLI * SNMP * Cloud |
| 8 | Zasilanie | Punkt dostępowy musi umożliwiać jego zasilanie z PoE,  Maksymalny pobór mocy nie może być większy niż 15,5 W |
| 9 | MTBF (hr) | Parametr te nie powinien być niższy niż 4,134,738 |
| 10 | Gwarancja | Urządzenie powinno być objęte ograniczoną dożywotnia gwarancją producenta |
| 11 | Serwis | W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje następnego dnia roboczego po tym, w którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat. |
| 12 | Wymagane Certyfikaty | FCC part 15C, FCC part 15E, ETSI EN 300 328, EN 301 893, LP0002  FCC Part 15B, EN 301 489-1, EN 301 489-17, EN55032, EN55024, EN61000-3-2/-3, BSMI CNS13438  EN 60950-1, IEC 60950-1, BSMI CNS14336-1 |
| 13 | Pozostałe | Sprzęt musi pochodzić z polskiego kanału dystrybucji |

# UTM

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa parametru** | **Wymagane parametry** |
| 1 | **Obudowa** | Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19” (w zestawie muszą znajdować się odpowiednie uchwyty). Obudowa urządzenia nie może być wyższa niż 1U. |
| 2 | **Zasilanie** | Maksymalna moc pobierana przez urządzenie nie może przekraczać 46W. |
| 3 | **Elementy mechaniczne** | Urządzenie nie może posiadać wbudowanego dysku/dysków twardych. |
| 4 | **Interfejsy** | Minimum 12 konfigurowalnych portów 10/100/1000 Mbps RJ-45, 2 konfigurowalne porty SFP, port konsoli (DB9) |
| 5 | **Tryby pracy** | Urządzenie musi umożliwiać konfigurację trybu router, trybu bridge oraz hybrydowo (router i bridge jednocześnie). Urządzenie musi mieć wbudowany kontroler do zarządzania infrastrukturą WIFI dla maksymalnie 264 punktów dostępowych. |
| 6 | **Obsługa łączy 3G** | Urządzenie musi posiadać co najmniej dwa porty USB 3.0 umożliwiające podłączenie adaptera 3G i realizację za pośrednictwem w/w adaptera łącza zapasowego. |
| 7 | **Protokoły Routingu** | Urządzenie musi wspierać routing statyczny, protokoły RIPv1/v2 oraz OSPF,BGP |
| 8 | **VLAN 802.1q** | Urządzenie musi umożliwiać kreowanie interfejsów VLAN 802.1q. Funkcjonalność ta musi być dostępna w standardzie (bez konieczności zakupu dodatkowych licencji/modułów)  Urządzenie powinno obsługiwać nie mniej niż 128 interfejsów VLAN |
| 9 | **Sandboxing** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalności sandboxing bez konieczności zakupu dodatkowych licencji/modułów |
| 10 | **Web Security** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalności web security bez konieczności zakupu dodatkowych licencji/modułów |
| 11 | **Application Security** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalności application security bez konieczności zakupu dodatkowych licencji/modułów |
| 12 | **Malware Blocker** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalności malware blocker bez konieczności zakupu dodatkowych licencji/modułów |
| 13 | **IDP** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalności IDP (bez konieczności zakupu dodatkowych licencji/modułów) |
| 14 | **Reputation Filter** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalności reputation filter (bez konieczności zakupu dodatkowych licencji/modułów) |
| 15 | **Geo Enforcer** | Urządzenie musi pozwalać na aktywację co najmniej rocznej licencji funkcjonalność geo enforcer (bez konieczności zakupu dodatkowych licencji/modułów) |
| 14 | **SSL (HTTPS) inspection** | Urządzenie musi pozwalać na aktywację funkcji SSL (HTTPS) inspection |
| 15 | **2-Factor Authentication** | Urządzenie musi pozwalać na aktywację funkcji 2-Factor Authentication |
| 16 | **Microsoft Azure/ Amazon VPC** | Urządzenie musi pozwalać na połączenie z churą Microsoft Azure lub Amazon VPC |
| 17 | **Link Aggregation (LAG)** | Urządzenie musi pozwalać na aktywację funkcji Link Aggregation (LAG) |
| 18 | **VPN** | Obsługa co najmniej 1000 równoczesnych połączeń IPSec VPN/L2TP.  Obsługa co najmniej 150 równoczesnych połączeń SSL VPN. Funkcjonalność ta musi być dostępna w standardzie (bez konieczności zakupu dodatkowych licencji/modułów).  Przepustowość VPN nie powinna być mniejsza niż 1200 Mbps |
| 19 | **Wysoka dostępność** | Urządzenie musi wspierać tryb wysokiej dostępności. W przypadku awarii głównego urządzenia, odpowiednio skonfigurowane urządzenie zapasowe musi przejąć obsługę sieci bez ingerencji administratora. |
| 20 | **Monitorowanie oraz raportowanie zdarzeń** | Musi istnieć możliwość zapisywania logów na nośniku USB lub dysku twardym podłączonym do urządzenia poprzez interfejs USB oraz wysyłania logów na zewnętrzne serwery syslog. W cenie urządzenia powinna być uwzględniona roczna licencja na aplikację chmurową przeznaczoną do analizowania logów i generowania raportów dotyczących funkcjonowania bramy. |
| 21 | **Kształtowanie Pasma** | Urządzenie musi umożliwiać elastyczne zarządzanie przepustowością, bezpośrednio na interfejsach jak i pozwalać na zdefiniowanie odpowiedniego pasma dla konkretnych portów i protokołów sieciowych.  W przypadku aktywnej licencji IDS/IDP musi istnieć również możliwość definiowania pasma dla wybranych aplikacji. |
| 22 | **Autoryzacja użytkowników** | Urządzenie powinno umożliwiać autoryację użytkowników w oparciu o wewnętrzną bazę użytkowników oraz zewętrzne serwery RADIUS, Microsoft AD, LDAP |
| 23 | **Wydajność** | Przepustowość dla firewall’a nie powinna być mniejsza niż 6000 Mbps  Przepustowość UTM (aktywowane moduły AV, IDP, Firewall) nie powinna być mniejsza niż 1500 Mbps |
| 24 | **Maksymalna liczba równoczesnych sesji** | Maksymalna liczba równolegle obsługiwanych sesji nie może być mniejsza niż 1 600 000. |
| 25 | **Gwarancja** | Minimum 5 lat gwarancji na oferowane urządzenie |
| 26 | **Serwis** | W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje następnego dnia roboczego po tym, w którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat. |
| 27 | **Inne** | Urządzenie musi być fabrycznie nowe i pochodzić z polskiego kanału dystrybucji |

# Oprogramowanie backupowe do serwerów

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Oprogramowanie backupowe do serwerów** | | |
| Wykonawca zobowiązany jest do dostarczenia w sumie 5 licencji oprogramowania do backupu serwerów z 3 letnią gwarancją. | | |
|  | **Wymagania techniczne dot. oprogramowania** | 1. Pełne wsparcie dla systemów rodziny Microsoft Windows Server: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012 R2 Essentials, Windows Server 2008 R2 Foundation, Windows Server 2008 Foundation z SP2 lub wyższy, Windows Server 2003, Windows Server 2003 R2, Windows 2000 Server/Advanced Server (SP4 lub nowszy),  2. Pełne wsparcie dla systemów rodziny Windows Small Business Server: Windows Server 2012 R2 (Essentials, Foundation), Windows Server 2012 (Essentials, Foundation), Windows Small Business Server 2011, Windows Small Business Server 2008 (Standard i Premium), Windows Server 2008 R2 Foundation, Windows Small Business Server 2003 i R2  3. Pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server, Oracle VirtualBox, Citrix XenServer, Linux KVM, ProxMox, Red Hat Enterprise Virtualization (RHEV), Stratos everRun.  4. Wsparcie dla 32 i 64-bitowych systemów Microsoft.  5. Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS.  6. Wsparcie dla dysków z tablicą partycji MBR oraz GPT  7. Pełne wsparcie dla systemów Ubuntu 14.04, 16.04, 18.04, CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Oracle Linux (wszystkie systemy 64-bitowe).  8. Wsparcie systemów plików: ext2, ext3, ext4, XFS.  9. Program i wsparcie techniczne dostępne w języku polskim |
|  | **Tworzenie kopii zapasowych (backupu)** | 1. Backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami. 2. Program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umożliwiać backup z częstotliwością min. co 15 minut. 3. Istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire. 4. Program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki. 5. Program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie. 6. Możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g. 7. Do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu. 8. Program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive’a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego. 9. Rozwiązanie pozwala na okresową weryfikacje, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać. 10. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi. 11. Podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu. 12. Program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email. 13. Program umożliwia konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX.   Program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP. |
|  | **Przywracanie z kopii zapasowych** | 1. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive’a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu.  2. Program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej, oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną.  3. Bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej.  4. Program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości.  5. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows.  6. Program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni. |
|  | **Zdalne zarządzanie** | 1. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej.  2. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej.  3. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych.  4. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych.  5. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej.  6. Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO. |

# Oprogramowanie do zarządzania infrastrukturą IT

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Oprogramowanie do zarządzania infrastrukturą IT** | | |
| 1. | **Specyfikacja techniczna Oprogramowania** | Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów.  Moduły mają umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.  Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.  Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta. |
| 2. | **Licencje** | Licencje dla nielimitowanej liczby urządzeń oraz możliwość zarządzanie do min. 35 stacjami roboczymi.  Aktualizacje i pomoc techniczna świadczona przez okres 1 roku. |
| 3. | **Monitorowanie infrastruktury** | Musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:  ✓ wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping).  ✓ wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci.  ✓ wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.  ✓ serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.  ✓ serwerów pocztowych:  - program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę,  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),  - program ma możliwość wykonywania operacji testowych,  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.  ✓ monitorowania serwerów WWW i adresów URL.  ✓ obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.  ✓ obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.  ✓ obsługi komunikatów syslog i pułapek SNMP.  ✓ monitoringu routerów i przełączników wg:  - zmian stanu interfejsów sieciowych,  - ruchu sieciowego,  - podłączonych stacji roboczych – graficzna prezentacja panelu switcha,  - ruchu generowanego przez podłączone do portów stacje robocze.  ✓ serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie /zatrzymanie/zrestartowanie.  ✓ wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. |
| 4. | **Inwentaryzacja** | Program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:  1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.  2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.  3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.  4. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.  5. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.  6. Umożliwia odczytanie numeru seryjnego (klucze licencyjne).  7. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.  8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.  9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie.  10. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.  Moduł inwentaryzacji sprzętu umożliwia prowadzenie bazy ewidencji majątku IT w zakresie:  ✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,  ✓ definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo istnieje możliwość importu danych z zewnętrznego źródła (.CSV),  ✓ generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania,  ✓ archiwizacji i porównywania audytów środków trwałych,  ✓ tworzenia kodów kreskowych w Środkach Trwałych,  ✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy,  ✓ inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android,  ✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),  ✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” ze szczegółów środków trwałych lub licencji  Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:  1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.  2. Zarządzanie posiadanymi licencjami.  3. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.  4. Zarządzanie posiadanymi licencjami: raport zgodności licencji.  5. Możliwość przypisania do programów numerów seryjnych, wartości itp. |
| 5. | **Aktywność użytkowników** | Program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:  ✓ Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),  ✓ Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,  ✓ Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,  ✓ Informacji o edytowanych przez użytkownika dokumentach,  ✓ Historii pracy (cykliczne zrzuty ekranowe),  ✓ Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),  ✓ Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),  ✓ Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,  ✓ Nagłówków przesyłanej poczty e-mail.  Program ponadto musi posiadać możliwość:  ✓ blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl),  ✓ blokowania ruchu na wskazanych portach TCP/IP,  ✓ blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,  ✓ wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,  ✓ przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika). |
| 6. | **Zdalna pomoc użytkownikom** | W ramach kontroli stacji użytkownika dostępny musi być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten zawiera również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.  Moduł pomocy zdalnej musi umożliwiać również:  ✓ pobieranie listy użytkowników z Active Directory,  ✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,  ✓ tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii),  ✓ przypisywanie pracowników helpdesk do kategorii zgłoszeń,  ✓ procesowanie zgłoszeń użytkowników z wiadomości e-mail,  ✓ tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,  ✓ wykonywanie operacji na wielu zgłoszeniach równocześnie,  ✓ dołączanie załączników do zgłoszeń,  ✓ zrzuty ekranowe (podgląd pulpitu),  ✓ dystrybucję oprogramowania przez Agentów,  ✓ dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),  ✓ zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,  ✓ możliwość skonfigurowania automatyzacji procesowania zgłoszeń,  ✓ planowanie nieobecności pracowników helpdesk,  ✓ obsługę umów o gwarantowanym poziomie świadczenia usług (SLA),  ✓ generowanie raportów obsługi helpdesk,  ✓ zdalne wykonywanie poleceń poprzez Agentów (np. utworzenie / edycja konta lokalnego użytkownika systemu),  ✓ zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),  ✓ wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików. |
| 7. | **Ochrona danych przed wyciekiem** | 1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.   Zarządzanie prawami dostępu do urządzeń:  1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.  2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane.  3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.  4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.  5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.  Audyt operacji na urządzeniach przenośnych:  1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.  2. Podłączenie/odłączenie urządzenia przenośnego.  Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. |

# System operacyjny

| **Lp.** | | **Nazwa komponentu** | | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- | --- | --- |
| **System operacyjny** | | | | |
|  | Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa:  - do każdego z dostarczanych serwerów kompletu licencji oprogramowania serwerowego systemu operacyjnego, ilość licencji 7 sztuk oraz  - licencji dostępowych, spełniających minimalne wymagania funkcjonalne określone poniżej oraz ich instalacja i konfiguracja.  Zamawiający wymaga licencji w wersji komercyjnej | | | |
|  |  | | Oprogramowanie serwerowe typu Windows Server 2019  lub równoważne\* | |
| 1. | Wymaganie ogólne | | Wykonawca dostarczy odpowiednią ilość licencji na serwerowy system operacyjny w licencjonowaniu komercyjnym: umożliwiające zainstalowanie na min. dwóch serwerach fizycznych, wyposażonych w dwa procesory 16 rdzeniowe każdy | |
| 2. | Wymaganie ogólne | | Licencja ma uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. | |
| 3. | Wymaganie ogólne | | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. | |
| 4. | Wymaganie ogólne | | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. | |
| 5. | Wymaganie ogólne | | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). | |
| 6. | Wymaganie ogólne | | Graficzny interfejs użytkownika. | |
| 7. | Wymaganie ogólne | | Obsługa systemów wieloprocesorowych. | |
| 8. | Wymaganie ogólne | | Obsługa platform sprzętowych x86, x64. | |
| 9. | Wymaganie ogólne | | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. | |
| 10. | Wymaganie ogólne | | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowego oprogramowani: | |
| 10.1. | Wymaganie ogólne | | Usługi sieciowe DNS i DHCP, | |
| 10.2. | Wymaganie ogólne | | Usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały), | |
| 10.3. | Wymaganie ogólne | | Zdalna dystrybucja oprogramowania na stacje robocze, | |
| 10.4. | Wymaganie ogólne | | Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, | |
| 10.5. | Wymaganie ogólne | | PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego), | |
| 10.6. | Wymaganie ogólne | | Szyfrowanie plików i folderów, szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), | |
| 10.7. | Wymaganie ogólne | | Możliwość rozłożenia obciążenia serwerów, | |
| 10.8. | Wymaganie ogólne | | Serwis udostępniania stron WWW, serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management), | |
| 10.9. | Wymaganie ogólne | | Wsparcie dla protokołu IP w wersji 6 (IPv6). | |
| 11. | Wymaganie ogólne | | Możliwość tworzenie serwerów wirtualnych, oprogramowanie wspierające tworzenie serwerów wirtualnych musi spełniać następujące wymagania funkcjonalne: | |
| 11.1. | Wymaganie ogólne | | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych, | |
| 11.2. | Wymaganie ogólne | | Licencja musi umożliwiać jej przenoszenie pomiędzy serwerami różnych producentów z zachowaniem gwarancji i zmianę wersji oprogramowania na niższą (downgrade), | |
| 11.3. | Wymaganie ogólne | | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze, | |
| 11.4. | Wymaganie ogólne | | Możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych, | |
| 11.5. | Wymaganie ogólne | | Możliwość przydzielania większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji, | |
| 11.6. | Wymaganie ogólne | | Możliwość udostępniania maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy, | |
| 11.7. | Wymaganie ogólne | | Konsola graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. | |
| 11.8. | Wymaganie ogólne | | Możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach | |
| 11.9. | Wymaganie ogólne | | Możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. | |
| 11.10. | Wymaganie ogólne | | Możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi | |
| 11.11. | Wymaganie ogólne | | Możliwość integracji z usługami katalogowymi Microsoft Active Directory. | |
| 11.12. | Wymaganie ogólne | | Mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn | |
| 11.13. | Wymaganie ogólne | | Obsługa przełączania ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku ścieżek. | |
| 11.14. | Wymaganie ogólne | | Możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, | |
| 11.15. | Wymaganie ogólne | | Mechanizm wysokiej dostępności HA, 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 | |
| 11.16. | Wymaganie ogólne | | 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. | |
| 11.17. | Wymaganie ogólne | | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej | |
| 11.18. | Wymaganie ogólne | | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN) | |
| 12. | Wymaganie ogólne | | Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym | |
| 13. | Wymaganie ogólne | | Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. | |
| 14. | Wymaganie ogólne | | Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych. | |
| 15. | Wymaganie ogólne | | Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. | |
| 16. | Wymaganie ogólne | | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. | |
| 17. | Wymaganie ogólne | | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane  w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. | |
| 18. | Wymaganie ogólne | | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. | |
| 19. | Wymaganie ogólne | | Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. | |
| 20. | Wymaganie ogólne | | Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. | |
|  |  | | Licencje dostępowe do oferowanego systemu serwerowego lub równoważne spełniające poniższe wymagania: | |
| 1. | Wymaganie ogólne | | Licencje serwerowego systemu operacyjnego muszą zostać dostarczone z licencjami dostępowymi do zasobów serwerowego systemu operacyjnego dla minimum 40 użytkowników ( licencje na użytkownika ). | |
|  | Wymagania w zakresie instalacji i konfiguracji | | | |
| 1. | Wymaganie ogólne | | Instalacja i konfiguracja na serwerach wirtualnych kontrolera domeny przy wykorzystaniu dostarczonych systemów operacyjnych w zakresie środowiska domeny. | |
| 2. | Wymaganie ogólne | | Instalacja niezbędnych usług serwerów, funkcjonalności kontrolera domeny (FQDN i NetBIOS name). | |
| 3. | Wymaganie ogólne | | Założenie kont administratorów niezbędnych do konfiguracji środowiska domenowego. | |
| 4. | Wymaganie ogólne | | Konfiguracja minimum 10 użytkowników domeny według wskazówek Zamawiającego. | |
| 5. | Wymaganie ogólne | | Konfiguracja definicji zasad grup według wskazówek Zamawiającego. | |
| 6. | Wymaganie ogólne | | Instalacja i konfiguracja na serwerze fizycznym zapasowego kontrolera domeny przy wykorzystaniu dostarczonych systemów operacyjnych w zakresie środowiska domeny. | |
| 7. | Wymaganie ogólne | | Konfiguracja usług do pracy w istniejącym środowisku sieciowym. | |
| 8. | Wymaganie ogólne | | Podłączenie do domeny. | |
| 9. | Wymaganie ogólne | | Instalację usług niezbędnych do funkcjonowania serwera jako zapasowy kontroler domeny. | |
| 10. | Wymaganie ogólne | | Podniesienie do rangi drugiego kontrolera domeny. | |
| 11. | Wymaganie ogólne | | Stworzenie udostępnionych udziałów sieciowych według wskazówek zamawiającego. | |
| 12. | Wymaganie ogólne | | Konfiguracja usług ról przestrzeni nazw systemu plików DFS i replikacji systemu plików DFS, które składają się na rozproszony system plików według wskazówek Zamawiającego. | |
|  |  | | Licencje usług pulpitu zdalnego kompatybilne z systemem operacyjnym  Typu Windows Server User CALL - spełniające poniższe wymagania: | |
|  | Wymaganie ogólne | | Licencje dostępu zdalnego muszą zostać dostarczone z licencjami dostępowymi do zasobów serwerowego systemu operacyjnego dla minimum 40 użytkowników ( licencje na użytkownika ). | |

# Szafa serwerowa RACK 42U operacyjny

| **Lp.** | | **Nazwa komponentu** | | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- | --- | --- |
| **System operacyjny** | | | | |
|  | Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa:  - szafy serwerowej w ilość - 1 sztuk | | | |
|  |  | | Szafa serwerowa RACK 19” | |
| 1. | Typ szafy / rodzaj | | Serwerowa RACK 19” stojąca | |
| 2. | Wysokość teleinformatyczna | | 42U | |
| 3. | Wysokość | | 2047,5 | |
| 4. | Szerokość | | 800 mm | |
| 5. | Głębokość | | 1200 mm | |
| 6. | Maksymalne statyczne obciążenie | | 800 kg | |
| 7. | Głębokość montażowa | | 1120 mm | |
| 8. | Ilość miejsc na wentylatory | | 4 | |
| 9. | Rodzaj drzwi przednich | | Przeszklone | |
| 10. | Rodzaj drzwi tylnych | | Metal | |
| 11. | Grubość bocznego panelu | | 1 mm | |
| 12. | Grubość szyn montażowych | | 2 mm | |
| 13. | Grubość pozostałych elementów | | 1,2 mm | |
| 14. | Akcesoria w zestawie | | Kółka z hamulcem, Nóżki, Panel Wentylacyjny (4 wentylatory), Śruby M6, Zamek przedni, Zamek tylny, Zamki boczne | |
| 15. | Standard | | ANSI/EIA RS-310-D, DIN 41491/PART 1, DIN 41494/PART 7, ETSI, IEC297-2:1982 | |

# \*Warunki równoważności

**W związku z posiadaną przez Zamawiającego architekturą** serwerową, sieciową i wdrożonym oprogramowaniem Zamawiający podaje wymagania na zamawiane niezbędne elementy używając parametrów posiadanej infrastruktury. Zamawiający dopuszcza dostawę elementów równoważnych o parametrach nie gorszych od wyżej wymienionych tj. o takich samych parametrach technicznych i jakościowych oraz w identycznym stopniu zapewniających kompatybilność. W przypadku dostawy urządzeń równoważnych o parametrach nie gorszych od wyżej wymienionych elementów, należy przewidzieć rozbudowę posiadanych przez Zamawiającego urządzeń, usług czy aplikacji. Udowodnienie tej równoważności, tj. pełnej kompatybilności oraz zgodności technicznych parametrów ilościowych i jakościowych jest obowiązkiem Wykonawcy, np. poprzez udokumentowanie tego faktu stosownym certyfikatem od producenta.

**\* 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 przedstawić na żądanie Zamawiającego 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.