Załącznik nr 2

**1. Poradnia Zdrowia Psychicznego w Malborku**

**1.1. Szafa 12U – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Wysokość wewnętrzna | 12 U |  |
| 2. | Wysokość | max. 635 mm |  |
| 3. | Szerokość | max. 600 mm |  |
| 4. | Głębokość | max. 600 mm |  |
| 5. | Masa netto | max. 23 kg |  |
| 6. | Maksymalna nośność | 60 kg |  |
| 7. | Dodatkowe wymagania | Typ szafy: Wisząca |  |
| Klasa szczelności: IP20 |  |
| Rodzaj drzwi: Szyba hartowana |  |
| Zgodność ze standardami: ANSI/EIA RS-310-D,IEC297-2,DIN41494; PART1 & PART7,ETSI |  |
| Materiał wykonania: Wysokiej jakości stal walcowana, malowana proszkowo |  |
| Wentylator: min. 120mm, 220V |  |
| Grubość blachy: Profil montażowy – min. 1,50mm, Reszta – min. 1,2mm |  |
| Otwory kablowe: Góra, Dół |  |
| Akcesoria do mocowania, zestaw do uziemienia, zamek drzwi przednich, |  |
| Dwa zamki paneli bocznych, min. 10 śrub M6. |  |
| Kolor czarny |  |
| Listwa zasilająca 19’’ min. 5 gniazd. |  |

**1.2. Przełącznik 24 porty POE – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Architektura sieci LAN | GigabitEthernet |  |
| 2. | SmartSwitch (WEB Managed) | Tak |  |
| 3. | Liczba portów 1000BaseT (RJ45) | min. 24 szt. |  |
| 4. | Liczba portów COMBO GEth (RJ45)/MiniGBIC (SFP) | min. 2 szt. |  |
| 5. | Zarządzanie, monitorowanie i konfiguracja | CLI - Command Line Interface |  |
| Zdalne zarządzanie |  |
| SNMP - Simple Network Management Protocol |  |
| CLI - Command Line Interface |  |
| IPv4 - Internet Protocol v4 (RFC 791) Upgradeable to v6 (RFC 1883) |  |
| DHCP Server - Dynamic Host Configuration Protocol (RFC 2131) |  |
| 6. | Protokoły uwierzytelniania i kontroli dostępu | SSH v.1 - Secure Shall ver. 1 |  |
| SSH v.2 - Secure Shall ver. 2 |  |
| SSL - Secure Sockets Layer |  |
| IEEE 802.1x - Network Login |  |
| RADIUS - zdalne uwierzytelnianie użytkowników |  |
| TACACS+ - Terminal Access Controller Access Control System |  |
| ACL bazujący na adresach MAC |  |
| ACL bazujący na sieciach VLAN |  |
| ACL bazujący na Diffserv (DSCP) |  |
| ACL bazujący na adresach IP i typie protokołu |  |
| ACL bazyjący na numerach portów TCP/UDP |  |
| ACL bazujący na protokole 802.1p |  |
| 7. | Obsługiwane protokoły i standardy | IEEE 802.3 - 10BaseT |  |
| IEEE 802.3u 100BASE-TX Fast Ethernet |  |
| IEEE 802.3ab - 1000BaseT |  |
| IEEE 802.3ad - Link Aggregation Control Protocol |  |
| IEEE 802.3z - 1000BaseSX/LX |  |
| IEEE 802.3x - Flow Control |  |
| IEEE 802.1D - Spanning Tree |  |
| IEEE 802.1Q - Virtual LANs |  |
| IEEE 802.1w - Rapid Convergence Spanning Tree |  |
| IEEE 802.1s - Multiple Spanning Tree |  |
| IEEE 802.1x - Network Login |  |
| IEEE 802.3af - Power over Ethernet |  |
| IEEE 802.3at - Power over Ethernet+ |  |
| IPv6 |  |
| ACL - Access Control List |  |
| QoS - Quality of Service (kontrola jakość usług i przepustowości) |  |
| IPv4 |  |
| DHCP - Dynamic Host Configuration Protocol |  |
| SSL - Secure Sockets Layer |  |
| SSH - Secure Shall |  |
| SNTP - Simple Network Time Protocol |  |
| TFTP - Trivial File Transfer Protocol |  |
| SNMP - Simple Network Management Protocol |  |
| TACACS+ |  |
| ToS - Type of service |  |
| WDR - Wide dynamic range |  |
| CoS - Class of Service |  |
| TCP |  |
| 8. | Rozmiar tablicy adresów MAC | min. 16384 |  |
| 9. | Warstwa przełączania | 2 |  |
| 10. | Typ obudowy | 1U Rack |  |
| 11. | Maksymalny pobór mocy | 180 Wat |  |
| 12. | Dodatkowe funkcje | zabezpieczenie przed atakami typu DoS (Denial of Service) |  |

**1.3. Firewall sprzętowy do zabezpieczenia sieci i połączeń VPN z centralą – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany****TAK/NIE** |
| 1. | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.  |  |
| 2. | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |
| 3. | Monitoring stanu realizowanych połączeń VPN.  |  |
| 4. | System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. |  |
| 5. | System realizujący funkcję Firewall powinien dysponować minimum 5 portami Ethernet 10/100/1000 Base-TX |  |
| 6. | System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| 7. | W zakresie Firewall’a obsługa nie mniej niż 800 tys. jednoczesnych połączeń oraz 12 tys. nowych połączeń na sekundę  |  |
| 8. | Przepustowość Firewall’a: nie mniej niż 0,9 Gbps |  |
| 9. | Wydajność szyfrowania VPN IPSec: nie mniej niż 70 Mbps |  |
| 10. | System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. |  |
| 11. | System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. |  |
| 12. | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: |  |
|          Kontrola dostępu - zapora ogniowa klasy Stateful Inspection |  |
| .         Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS  |  |
|          Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN |  |
|          Ochrona przed atakami - Intrusion Prevention System |  |
|          Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.  |  |
|          Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP |  |
|          Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma  |  |
|          Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) |  |
|          Możliwość analizy ruchu szyfrowanego protokołem SSL |  |
|          Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) |  |
| 13. | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 500 Mbps |  |
| 14. | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 150 Mbps |  |
| 15. | W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: |  |
|          Tworzenie połączeń w topologii Site-to-site oraz Client-to-site |  |
|          Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności  |  |
|          Praca w topologii Hub and Spoke oraz Mesh |  |
|          Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF |  |
|       Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth |  |
| 16. | W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.  |  |
| 17. | Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.  |  |
| 18. | Translacja adresów NAT adresu źródłowego i docelowego. |  |
| 19. | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.  |  |
| 20. | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ |  |
| 21. | Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) ) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. |  |
| 22. | Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. |  |
| 23. | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP |  |
| 24. | Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.  |  |
| 25. | Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. |  |
| 26. | System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: |  |
|          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  |  |
|          Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory |  |
| 27. | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: |  |
|          ICSA lub EAL4 dla funkcji Firewall |  |
|          ICSA lub NSS Labs dla funkcji IPS |  |
|          ICSA dla funkcji: SSL VPN, IPSec VPN |  |
| 28. | Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| 29. | Serwisy i licencje - w ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 3 lat. |  |
| 30. | Gwarancja oraz wsparcie - System powinien być objęty serwisem gwarancyjnym producenta przez okres min. 2 lat, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. |  |

**1.4. UPS 1500VA do podtrzymana urządzeń – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Moc pozorna | min. 1500 VA |  |
| 2. | Moc rzeczywista | min. 1000 Wat |  |
| 3. | Architektura UPSa | line-interactive |  |
| 4. | Maks. czas przełączenia na baterię | 4 ms |  |
| 5. | Liczba i rodzaj gniazdek z utrzymaniem zasilania | min. 4 x French |  |
| 6. | Liczba, typ gniazd wyj. z ochroną antyprzepięciową | min. 4 x French |  |
| 7. | Typ gniazda wejściowego | IEC320 C14 (10A) |  |
| 8. | Czas podtrzymania dla obciążenia 100% | min. 4 min |  |
| 9. | Czas podtrzymania przy obciążeniu 50% | min. 9 min |  |
| 10. | Zakres napięcia wejściowego w trybie podstawowym | 165-285 V |  |
| 11. | Zimny start | Tak |  |
| 12. | Układ automatycznej regulacji napięcia (AVR) | Tak |  |
| 13. | Sinus podczas pracy na baterii | Nie |  |
| 14. | Porty komunikacji | min. USB |  |
|  15. | Port zabezpieczający linie danych | RJ11 - linia modemowa/faxowa, DSL |  |
| RJ45 - linia 10/100/1000BaseT |  |
|  16. | Diody sygnalizacyjne | Wyświetlacz LCD |  |
|  17. | Typ obudowy | 1U Rack |  |
|  18. | Wyposażenie standardowe | oprogramowanie na CD |  |
| Kabel USB |  |
|  19. | Dołączone oprogramowanie | Płyta ze sterownikami |  |
|  20. | Gwarancja | min. 24 miesięce |  |

**1.5. Access Point do budowy sieci WiFi – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Rodzaj obudowy | Pokojowa |  |
| 2. | RAM | min. 1 GB |  |
| 3. | Pamięć fleszowa | min. 256 MB |  |
| 4. | Protokół komunikacyjny danych | IEEE 802.11b,IEEE 802.11a,IEEE 802.11g,IEEE 802.11n,IEEE 802.11ac (draft 5.0) |  |
| 5. | Pasmo częstotliwości | 2.4 GHz,5 GHz |  |
| 6. | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 7. | Zasilanie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 8. | Wymiary (szer./głęb./wys.) | max. 21.08 cm x 21.08 cm x 50.8 cm |  |
| 9. | Waga | max. 1.41 kg |  |
| 10. | Antena | Wewnętrzna |  |
| 11. | Kierunkowość | Antena dookólna |  |
| 12. | Poziom uzyskany | min.5 dBi |  |
| 13. | Interfejsy | 1 x 1000Base-T (PoE+) - RJ-45  |  |
| 1 x konsola - RJ-45  |  |
| 1 x USB 2.0 - Type A |  |
| 14. | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 15. | Zasilacz | Adapter mocy zewnętrznej |  |
| 16. | Wymagane napięcie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 17. | Zużycie energii w trybie aktywności | max. 16 wat |  |
| 18. | Wymaganie dodatkowe | w celu wspólnego zarządzania, tego samego producenta co przełącznik |  |
| 19. | Gwarancja | min. 24 miesięce on site NBD |  |

**2. Poradnia Leczenia Uzależnienia od Alkoholu w Sztumie**

**2.1. Szafa 12U – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Wysokość wewnętrzna | 12 U |  |
| 2. | Wysokość | max. 635 mm |  |
| 3. | Szerokość | max. 600 mm |  |
| 4. | Głębokość | max. 600 mm |  |
| 5. | Masa netto | max. 23 kg |  |
| 6. | Maksymalna nośność | 60 kg |  |
| 7. | Dodatkowe wymagania | Typ szafy: Wisząca |  |
| Klasa szczelności: IP20 |  |
| Rodzaj drzwi: Szyba hartowana |  |
| Zgodność ze standardami: ANSI/EIA RS-310-D,IEC2972,DIN41494; PART1 & PART7,ETSI |  |
| Materiał wykonania: Wysokiej jakości stal walcowana, malowana proszkowo |  |
| Wentylator: min. 120mm, 220V |  |
| Grubość blachy: Profil montażowy – min. 1,50mm, Reszta – min. 1,2mm |  |
| Otwory kablowe: Góra, Dół |  |
| Akcesoria do mocowania, zestaw do uziemienia, zamek drzwi przednich, |  |
| Dwa zamki paneli bocznych, min. 10 śrub M6. |  |
| Kolor czarny |  |
| Listwa zasilająca 19’’ min 5 gniazd. |  |

**2.2. Przełącznik 24 porty POE – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Architektura sieci LAN | GigabitEthernet |  |
| 2. | SmartSwitch (WEB Managed) | Tak |  |
| 3. | Liczba portów 1000BaseT (RJ45) | min. 24 szt. |  |
| 4. | Liczba portów COMBO GEth (RJ45)/MiniGBIC (SFP) | min. 2 szt. |  |
| 5. | Zarządzanie, monitorowanie i konfiguracja | CLI - Command Line Interface |  |
| Zdalne zarządzanie |  |
| SNMP - Simple Network Management Protocol |  |
| CLI - Command Line Interface |  |
| IPv4 - Internet Protocol v4 (RFC 791) Upgradeable to v6 (RFC 1883) |  |
| DHCP Server - Dynamic Host Configuration Protocol (RFC 2131) |  |
| 6. | Protokoły uwierzytelniania i kontroli dostępu | SSH v.1 - Secure Shall ver. 1 |  |
| SSH v.2 - Secure Shall ver. 2 |  |
| SSL - Secure Sockets Layer |  |
| IEEE 802.1x - Network Login |  |
| RADIUS - zdalne uwierzytelnianie użytkowników |  |
| TACACS+ - Terminal Access Controller Access Control System |  |
| ACL bazujący na adresach MAC |  |
| ACL bazujący na sieciach VLAN |  |
| ACL bazujący na Diffserv (DSCP) |  |
| ACL bazujący na adresach IP i typie protokołu |  |
| ACL bazyjący na numerach portów TCP/UDP |  |
| ACL bazujący na protokole 802.1p |  |
| 7. | Obsługiwane protokoły i standardy | IEEE 802.3 - 10BaseT |  |
| IEEE 802.3u 100BASE-TX Fast Ethernet |  |
| IEEE 802.3ab - 1000BaseT |  |
| IEEE 802.3ad - Link Aggregation Control Protocol |  |
| IEEE 802.3z - 1000BaseSX/LX |  |
| IEEE 802.3x - Flow Control |  |
| IEEE 802.1D - Spanning Tree |  |
| IEEE 802.1Q - Virtual LANs |  |
| IEEE 802.1w - Rapid Convergence Spanning Tree |  |
| IEEE 802.1s - Multiple Spanning Tree |  |
| IEEE 802.1x - Network Login |  |
| IEEE 802.3af - Power over Ethernet |  |
| IEEE 802.3at - Power over Ethernet+ |  |
| IPv6 |  |
| ACL - Access Control List |  |
| QoS - Quality of Service (kontrola jakość usług i przepustowości) |  |
| IPv4 |  |
| DHCP - Dynamic Host Configuration Protocol |  |
| SSL - Secure Sockets Layer |  |
| SSH - Secure Shall |  |
| SNTP - Simple Network Time Protocol |  |
| TFTP - Trivial File Transfer Protocol |  |
| SNMP - Simple Network Management Protocol |  |
| TACACS+ |  |
| ToS - Type of service |  |
| WDR - Wide dynamic range |  |
| CoS - Class of Service |  |
| TCP |  |
| 8. | Rozmiar tablicy adresów MAC | min. 16384 |  |
| 9. | Warstwa przełączania | 2 |  |
| 10. | Typ obudowy | 1U Rack |  |
| 11. | Maksymalny pobór mocy | 180 Wat |  |
| 12. | Dodatkowe funkcje | zabezpieczenie przed atakami typu DoS (Denial of Service) |  |
| 13. | Gwarancja | min. 2 lata on site NBD |  |

**2.3. Firewall sprzętowy do zabezpieczenia sieci i połączeń VPN z centralą – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany****TAK/NIE** |
| 1 | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.  |  |
| 2 | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |
| 3 | Monitoring stanu realizowanych połączeń VPN.  |  |
| 4 | System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. |  |
| 5 | System realizujący funkcję Firewall powinien dysponować minimum 5 portami Ethernet 10/100/1000 Base-TX |  |
| 6 | System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| 7 | W zakresie Firewall’a obsługa nie mniej niż 800 tys. jednoczesnych połączeń oraz 12 tys. nowych połączeń na sekundę  |  |
| 8 | Przepustowość Firewall’a: nie mniej niż 0,9 Gbps |  |
| 9 | Wydajność szyfrowania VPN IPSec: nie mniej niż 70 Mbps |  |
| 10 | System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. |  |
| 11 | System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. |  |
| 7 | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: |  |
|          Kontrola dostępu - zapora ogniowa klasy Stateful Inspection |  |
|          Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS  |  |
|          Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN |  |
|          Ochrona przed atakami - Intrusion Prevention System |  |
|          Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.  |  |
|          Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP |  |
|          Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma  |  |
|          Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) |  |
|          Możliwość analizy ruchu szyfrowanego protokołem SSL |  |
|          Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) |  |
| 7 | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 500 Mbps |  |
| 9 | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 150 Mbps |  |
| 10 | W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: |  |
|          Tworzenie połączeń w topologii Site-to-site oraz Client-to-site |  |
|          Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności  |  |
|          Praca w topologii Hub and Spoke oraz Mesh |  |
|          Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF |  |
| ·        Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth |  |
| 11 | W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.  |  |
| 12 | Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.  |  |
| 13 | Translacja adresów NAT adresu źródłowego i docelowego. |  |
| 14 | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.  |  |
| 15 | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ |  |
| 16 | Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) ) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. |  |
| 17 | Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. |  |
| 18 | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP |  |
| 19 | Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.  |  |
| 20 | Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. |  |
| 21 | System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: |  |
|          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  |  |
|          Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory |  |
| 22 | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: |  |
|          ICSA lub EAL4 dla funkcji Firewall |  |
|          ICSA lub NSS Labs dla funkcji IPS |  |
|          ICSA dla funkcji: SSL VPN, IPSec VPN |  |
| 23 | Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| 24 | Serwisy i licencje - w ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 3 lat. |  |
| 25 | Gwarancja oraz wsparcie - System powinien być objęty serwisem gwarancyjnym producenta przez okres min. 2 lat, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. |  |

**2.4. UPS 1500VA do podtrzymana urządzeń – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Moc pozorna | min. 1500 VA |  |
| 2. | Moc rzeczywista | min. 1000 Wat |  |
| 3. | Architektura UPSa | line-interactive |  |
| 4. | Maks. czas przełączenia na baterię | 4 ms |  |
| 5. | Liczba i rodzaj gniazdek z utrzymaniem zasilania | min. 4 x French |  |
| 6. | Liczba, typ gniazd wyj. z ochroną antyprzepięciową | min. 4 x French |  |
| 7. | Typ gniazda wejściowego | IEC320 C14 (10A) |  |
| 8. | Czas podtrzymania dla obciążenia 100% | min. 4 min |  |
| 9. | Czas podtrzymania przy obciążeniu 50% | min. 9 min |  |
| 10. | Zakres napięcia wejściowego w trybie podstawowym | 165-285 V |  |
| 11. | Zimny start | Tak |  |
| 12. | Układ automatycznej regulacji napięcia (AVR) | Tak |  |
| 13. | Sinus podczas pracy na baterii | Nie |  |
| 14. | Porty komunikacji | min. USB |  |
|  15. | Port zabezpieczający linie danych | RJ11 - linia modemowa/faxowa, DSL |  |
| RJ45 - linia 10/100/1000BaseT |  |
|  16. | Diody sygnalizacyjne | Wyświetlacz LCD |  |
|  17. | Typ obudowy | 1U Rack |  |
|  18. | Wyposażenie standardowe | oprogramowanie na CD |  |
| Kabel USB |  |
|  19. | Dołączone oprogramowanie | Płyta ze sterownikami |  |
|  20. | Gwarancja | min. 24 miesięce |  |

**2.5. Access Point do budowy sieci WiFi – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Rodzaj obudowy | Pokojowa |  |
| 2. | RAM | min. 1 GB |  |
| 3. | Pamięć fleszowa | min. 256 MB |  |
| 4. | Protokół komunikacyjny danych | IEEE 802.11b,IEEE 802.11a,IEEE 802.11g,IEEE 802.11n,IEEE 802.11ac (draft 5.0) |  |
| 5. | Pasmo częstotliwości | 2.4 GHz,5 GHz |  |
| 6. | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 7. | Zasilanie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 8. | Wymiary (szer./głęb./wys.) | max. 1.08 cm x 21.08 cm x 50.8 cm |  |
| 9. | Waga | max. 1.41 kg |  |
| 10. | Antena | Wewnętrzna |  |
| 11. | Kierunkowość | Antena dookólna |  |
| 12. | Poziom uzyskany | min. 5 dBi |  |
| 13. | Interfejsy | 1 x 1000Base-T (PoE+) - RJ-45  |  |
| 1 x konsola - RJ-45  |  |
| 1 x USB 2.0 - Type A |  |
| 14. | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 15. | Zasilacz | Adapter mocy zewnętrznej |  |
| 16. | Wymagane napięcie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 17. | Zużycie energii w trybie aktywności | max. 16 wat |  |
| 18. | Wymaganie dodatkowe | w celu wspólnego zarządzania, tego samego producenta co przełącznik |  |
| 19. | Gwarancja | min. 24 miesięce on site NBD |  |

**3. Poradnia Zdrowia Psychicznego w Kwidzynie**

**3.1. Szafa 12U – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Wysokość wewnętrzna | 12 U |  |
| 2 | Wysokość | max. 635 mm |  |
| 3 | Szerokość | max. 600 mm |  |
| 4 | Głębokość | max. 600 mm |  |
| 5 | Masa netto | max. 23 kg |  |
| 6 | Maksymalna nośność | 60 kg |  |
| 7 | Dodatkowe wymagania | Typ szafy: Wisząca |  |
| Klasa szczelności: IP20 |  |
| Rodzaj drzwi: Szyba hartowana |  |
| Zgodność ze standardami: ANSI/EIA RS-310-D,IEC297-2,DIN41494; PART1 & PART7,ETSI |  |
| Materiał wykonania: Wysokiej jakości stal walcowana, malowana proszkowo |  |
| Wentylator: min. 120mm, 220V |  |
| Grubość blachy: Profil montażowy – min. 1,50mm, Reszta – min. 1,2mm |  |
| Otwory kablowe: Góra, Dół |  |
| Akcesoria do mocowania, zestaw do uziemienia, zamek drzwi przednich, |  |
| Dwa zamki paneli bocznych, min. 10 śrub M6. |  |
| Kolor czarny |  |
| Listwa zasilająca 19’’ min 5 gniazd. |  |

**3.2. Przełącznik 24 porty POE – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Architektura sieci LAN | GigabitEthernet |  |
| 2. | SmartSwitch (WEB Managed) | Tak |  |
| 3. | Liczba portów 1000BaseT (RJ45) | min. 24 szt. |  |
| 4. | Liczba portów COMBO GEth (RJ45)/MiniGBIC (SFP) | min. 2 szt. |  |
| 5. | Zarządzanie, monitorowanie i konfiguracja | CLI - Command Line Interface |  |
| Zdalne zarządzanie |  |
| SNMP - Simple Network Management Protocol |  |
| CLI - Command Line Interface |  |
| IPv4 - Internet Protocol v4 (RFC 791) Upgradeable to v6 (RFC1883) |  |
| DHCP Server - Dynamic Host Configuration Protocol (RFC2131) |  |
| 6. | Protokoły uwierzytelniania i kontroli dostępu | SSH v.1 - Secure Shall ver. 1 |  |
| SSH v.2 - Secure Shall ver. 2 |  |
| SSL - Secure Sockets Layer |  |
| IEEE 802.1x - Network Login |  |
| RADIUS - zdalne uwierzytelnianie użytkowników |  |
| TACACS+ - Terminal Access Controller Access Control System |  |
| ACL bazujący na adresach MAC |  |
| ACL bazujący na sieciach VLAN |  |
| ACL bazujący na Diffserv (DSCP) |  |
| ACL bazujący na adresach IP i typie protokołu |  |
| ACL bazyjący na numerach portów TCP/UDP |  |
| ACL bazujący na protokole 802.1p |  |
| 7. | Obsługiwane protokoły i standardy | IEEE 802.3 - 10BaseT |  |
| IEEE 802.3u 100BASE-TX Fast Ethernet |  |
| IEEE 802.3ab - 1000BaseT |  |
| IEEE 802.3ad - Link Aggregation Control Protocol |  |
| IEEE 802.3z - 1000BaseSX/LX |  |
| IEEE 802.3x - Flow Control |  |
| IEEE 802.1D - Spanning Tree |  |
| IEEE 802.1Q - Virtual LANs |  |
| IEEE 802.1w - Rapid Convergence Spanning Tree |  |
| IEEE 802.1s - Multiple Spanning Tree |  |
| IEEE 802.1x - Network Login |  |
| IEEE 802.3af - Power over Ethernet |  |
| IEEE 802.3at - Power over Ethernet+ |  |
| IPv6 |  |
| ACL - Access Control List |  |
| QoS - Quality of Service (kontrola jakość usług iprzepustowości) |  |
| IPv4 |  |
| DHCP - Dynamic Host Configuration Protocol |  |
| SSL - Secure Sockets Layer |  |
| SSH - Secure Shall |  |
| SNTP - Simple Network Time Protocol |  |
| TFTP - Trivial File Transfer Protocol |  |
| SNMP - Simple Network Management Protocol |  |
| TACACS+ |  |
| ToS - Type of service |  |
| WDR - Wide dynamic range |  |
| CoS - Class of Service |  |
| TCP |  |
| 8. | Rozmiar tablicy adresów MAC | min. 16384 |  |
| 9. | Warstwa przełączania | 2 |  |
| 10. | Typ obudowy | 1U Rack |  |
| 11. | Maksymalny pobór mocy |  180 Wat |  |
| 12. | Dodatkowe funkcje | zabezpieczenie przed atakami typu DoS (Denial of Service) |  |
| 13. | Gwarancja | min. 2 lata on site NBD |  |

**3.3.Firewall sprzętowy do zabezpieczenia sieci i połączeń VPN z centralą – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.  |  |
| 2. | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |
| 3. | Monitoring stanu realizowanych połączeń VPN.  |  |
| 4. | System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. |  |
| 5. | System realizujący funkcję Firewall powinien dysponować minimum 5 portami Ethernet 10/100/1000 Base-TX |  |
| 6. | System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| 7. | W zakresie Firewall’a obsługa nie mniej niż 800 tys. jednoczesnych połączeń oraz 12 tys. nowych połączeń na sekundę  |  |
| 8. | Przepustowość Firewall’a: nie mniej niż 0,9 Gbps |  |
| 9. | Wydajność szyfrowania VPN IPSec: nie mniej niż 70 Mbps |  |
| 10. | System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. |  |
| 11. | System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. |  |
| 12. | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: |  |
|          Kontrola dostępu - zapora ogniowa klasy Stateful Inspection |  |
|          Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS  |  |
|          Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN |  |
|          Ochrona przed atakami - Intrusion Prevention System |  |
|          Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.  |  |
|          Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP |  |
| .         Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma  |  |
|          Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) |  |
|          Możliwość analizy ruchu szyfrowanego protokołem SSL |  |
|          Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) |  |
| 13. | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 500 Mbps |  |
| 14. | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 150 Mbps |  |
| 15. | W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: |  |
|          Tworzenie połączeń w topologii Site-to-site oraz Client-to-site |  |
|          Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności  |  |
|          Praca w topologii Hub and Spoke oraz Mesh |  |
|          Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF |  |
| ·        Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth |  |
| 16. | W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.  |  |
| 17. | Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.  |  |
| 18. | Translacja adresów NAT adresu źródłowego i docelowego. |  |
| 19. | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.  |  |
| 20. | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ |  |
| 21. | Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) ) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. |  |
| 22. | Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. |  |
| 23. | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP |  |
| 24. | Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.  |  |
| 25. | Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. |  |
| 26. | System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: |  |
|          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  |  |
|          Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory |  |
| 27. | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: |  |
|          ICSA lub EAL4 dla funkcji Firewall |  |
|          ICSA lub NSS Labs dla funkcji IPS |  |
|          ICSA dla funkcji: SSL VPN, IPSec VPN |  |
| 28. | Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| 29. | Serwisy i licencje - w ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 3 lat. |  |
| 30. | Gwarancja oraz wsparcie - System powinien być objęty serwisem gwarancyjnym producenta przez okres min. 2 lat, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. |  |

**3.4. UPS 1500VA do podtrzymana urządzeń – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Moc pozorna | min. 1500 VA |  |
| 2. | Moc rzeczywista | min. 1000 Wat |  |
| 3. | Architektura UPSa | line-interactive |  |
| 4. | Maks. czas przełączenia na baterię | 4 ms |  |
| 5. | Liczba i rodzaj gniazdek z utrzymaniem zasilania | min. 4 x French |  |
| 6. | Liczba, typ gniazd wyj. z ochroną antyprzepięciową | min. 4 x French |  |
| 7. | Typ gniazda wejściowego | IEC320 C14 (10A) |  |
| 8. | Czas podtrzymania dla obciążenia 100% | min. 4 min |  |
| 9. | Czas podtrzymania przy obciążeniu 50% | min. 9 min |  |
| 10. | Zakres napięcia wejściowego w trybie podstawowym | 165-285 V |  |
| 11. | Zimny start | Tak |  |
| 12. | Układ automatycznej regulacji napięcia (AVR) | Tak |  |
| 13. | Sinus podczas pracy na baterii | Nie |  |
| 14. | Porty komunikacji | min. USB |  |
|  15. | Port zabezpieczający linie danych | RJ11 - linia modemowa/faxowa, DSL |  |
| RJ45 - linia 10/100/1000BaseT |  |
|  16. | Diody sygnalizacyjne | Wyświetlacz LCD |  |
|  17. | Typ obudowy | 1U Rack |  |
|  18. | Wyposażenie standardowe | oprogramowanie na CD |  |
| Kabel USB |  |
|  19. | Dołączone oprogramowanie | Płyta ze sterownikami |  |
|  20. | Gwarancja | min. 24 miesięce |  |

**3.5. Access Point do budowy sieci WiFi – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Rodzaj obudowy | Pokojowa |  |
| 2 | RAM | min. 1 GB |  |
| 3 | Pamięć fleszowa | min. 256 MB |  |
| 4 | Protokół komunikacyjny danych | IEEE 802.11b,IEEE 802.11a,IEEE 802.11g,IEEE 802.11n,IEEE 802.11ac (draft 5.0) |  |
| 5 | Pasmo częstotliwości | 2.4 GHz,5 GHz |  |
| 6 | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 7 | Zasilanie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 8 | Wymiary (szer./głęb./wys.) | max. 21.08 cm x 21.08 cm x 50.8 cm |  |
| 9 | Waga | max. 1.41 kg |  |
| 10 | Antena | Wewnętrzna |  |
| 11 | Kierunkowość | Antena dookólna |  |
| 12 | Poziom uzyskany | min. 5 dBi |  |
| 13 | Interfejsy | 1 x 1000Base-T (PoE+) - RJ-45  |  |
| 1 x konsola - RJ-45  |  |
| 1 x USB 2.0 - Type A |  |
| 14 | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 15 | Zasilacz | Adapter mocy zewnętrznej |  |
| 16 | Wymagane napięcie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 17 | Zużycie energii w trybie aktywności | max. 16 wat |  |
| 18 | Wymaganie dodatkowe | w celu wspólnego zarządzania, tego samego producenta co przełącznik |  |
| 19 | Gwarancja | min. 24 miesięce on site NBD |  |

**4. Szpital Psychiatryczny w Prabutach**

**4.1. Szafa 42U – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Wysokość wewnętrzna | 42 U |  |
| 2. | Szerokość | max. 600 mm |  |
| 3. | Głębokość | max. 1000 mm |  |
| 4. | Masa netto | max. 125 kg |  |
| 5. | Maksymalna nośność | 800 kg |  |
| 6. | Dodatkowe wymagania | Typ szafy: stojąca |  |
| Klasa szczelności: IP20 |  |
| Rodzaj drzwi: Szyba hartowana |  |
| Zgodność ze standardami: ANSI/EIA RS-310-D,IEC297-2,DIN41494; PART1 & PART7,ETSI |  |
| Materiał wykonania: Wysokiej jakości stal walcowana, malowana proszkowo |  |
| Wentylator: min. 4x120mm, 220V |  |
| Grubość blachy: Profil montażowy – min. 2mm,  |  |
| Otwory kablowe: Góra, Dół |  |
| Akcesoria do mocowania, zestaw do uziemienia, zamek drzwi przednich, |  |
| Dwa zamki paneli bocznych,  |  |
| Kolor czarny |  |
| Listwa zasilająca 19’’ min 8 gniazd – 2 szt. |  |

Szafę należy zamontować w pomieszczeniu serwerowni i wyposażyć w sprzęt zakupiony w ramach tego samego postępowania. Dodatkowo należy w pomieszczeniu serwerowni należy wymienić drzwi na drzwi zewnętrzne antywłamaniowe.

**4.2. Przełącznik 52 porty POE – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Architektura sieci LAN | GigabitEthernet |  |
| 2. | SmartSwitch (WEB Managed) | Tak |  |
| 3. | Liczba portów 1000BaseT (RJ45) | min. 50 szt. |  |
| 4. | Liczba portów COMBO GEth (RJ45)/MiniGBIC (SFP) | min. 2 szt. |  |
| 5. | Zarządzanie, monitorowanie i konfiguracja | CLI - Command Line Interface |  |
| Zdalne zarządzanie |  |
| SNMP - Simple Network Management Protocol |  |
| CLI - Command Line Interface |  |
| IPv4 - Internet Protocol v4 (RFC 791) Upgradeable to v6 (RFC 1883) |  |
| DHCP Server - Dynamic Host Configuration Protocol (RFC 2131) |  |
| 6. | Protokoły uwierzytelniania i kontroli dostępu | SSH v.1 - Secure Shall ver. 1 |  |
| SSH v.2 - Secure Shall ver. 2 |  |
| SSL - Secure Sockets Layer |  |
| IEEE 802.1x - Network Login |  |
| RADIUS - zdalne uwierzytelnianie użytkowników |  |
| TACACS+ - Terminal Access Controller Access Control System |  |
| ACL bazujący na adresach MAC |  |
| ACL bazujący na sieciach VLAN |  |
| ACL bazujący na Diffserv (DSCP) |  |
| ACL bazujący na adresach IP i typie protokołu |  |
| ACL bazyjący na numerach portów TCP/UDP |  |
| ACL bazujący na protokole 802.1p |  |
| 7. | Obsługiwane protokoły i standardy | IEEE 802.3 - 10BaseT |  |
| IEEE 802.3u 100BASE-TX Fast Ethernet |  |
| IEEE 802.3ab - 1000BaseT |  |
| IEEE 802.3ad - Link Aggregation Control Protocol |  |
| IEEE 802.3z - 1000BaseSX/LX |  |
| IEEE 802.3x - Flow Control |  |
| IEEE 802.1D - Spanning Tree |  |
| IEEE 802.1Q - Virtual LANs |  |
| IEEE 802.1w - Rapid Convergence Spanning Tree |  |
| IEEE 802.1s - Multiple Spanning Tree |  |
| IEEE 802.1x - Network Login |  |
| IEEE 802.3af - Power over Ethernet |  |
| IEEE 802.3at - Power over Ethernet+ |  |
| IPv6 |  |
| ACL - Access Control List |  |
| QoS - Quality of Service (kontrola jakość usług iprzepustowości) |  |
| IPv4 |  |
| DHCP - Dynamic Host Configuration Protocol |  |
| SSL - Secure Sockets Layer |  |
| SSH - Secure Shall |  |
| SNTP - Simple Network Time Protocol |  |
| TFTP - Trivial File Transfer Protocol |  |
| SNMP - Simple Network Management Protocol |  |
| TACACS+ |  |
| ToS - Type of service |  |
| WDR - Wide dynamic range |  |
| CoS - Class of Service |  |
| TCP |  |
| 8. | Rozmiar tablicy adresów MAC | min. 8192 |  |
| 9. | Algorytm przełączania | Store-and-Forward |  |
| 10. | Prędkość magistrali wew. | min. 104 Gb/s |  |
| 11. | Przepustowość | min. 77,38 mpps |  |
| 12. | Bufor pamięci | min. 16 MB |  |
| 13. | Warstwa przełączania | 3 |  |
| 14. | Typ obudowy | rack 19" |  |
| 15. | Maksymalny pobór mocy | 461 Wat |  |
| 16. | Gwarancja | min. 2 lata on site NBD |  |

**4.3.Firewall sprzętowy do zabezpieczenia sieci i połączeń VPN z poradniami – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany.** |
| 1. | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.  |  |
| 2. | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |
| 3. | Monitoring stanu realizowanych połączeń VPN.  |  |
| 4. | System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. |  |
| 5. | System realizujący funkcję Firewall powinien dysponować minimum 4 portami Ethernet 10/100/1000 Base-TX |  |
| 6. | System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| 7. | W zakresie Firewall’a obsługa nie mniej niż 1,4 mln jednoczesnych połączeń oraz 22 tys. nowych połączeń na sekundę  |  |
| 8. | Przepustowość Firewall’a: nie mniej niż 1,2 Gbps |  |
| 9. | Wydajność szyfrowania VPN IPSec: nie mniej niż 200 Mbps |  |
| 10. | System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. |  |
| 11. | System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. |  |
| 11. | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: |  |
|          Kontrola dostępu - zapora ogniowa klasy Stateful Inspection |  |
|          Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS  |  |
|          Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN |  |
|          Ochrona przed atakami - Intrusion Prevention System |  |
|          Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.  |  |
|          Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP |  |
|          Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma  |  |
| .         Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) |  |
|          Możliwość analizy ruchu szyfrowanego protokołem SSL |  |
|          Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) |  |
| 12. | Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 750 Mbps |  |
| 13. | Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 190 Mbps |  |
| 14. | W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: |  |
|          Tworzenie połączeń w topologii Site-to-site oraz Client-to-site |  |
|          Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności  |  |
|          Praca w topologii Hub and Spoke oraz Mesh |  |
|          Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF |  |
| ·        Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth |  |
| 15. | W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.  |  |
| 16. | Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.  |  |
| 17. | Translacja adresów NAT adresu źródłowego i docelowego. |  |
| 18. | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.  |  |
| 19. | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ |  |
| 20. | Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) ) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. |  |
| 21. | Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. |  |
| 22. | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP |  |
| 23. | Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.  |  |
| 24. | Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. |  |
| 25. | System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: |  |
|          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  |  |
|          Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory |  |
| 26. | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: |  |
|          ICSA lub EAL4 dla funkcji Firewall |  |
|          ICSA lub NSS Labs dla funkcji IPS |  |
|          ICSA dla funkcji: SSL VPN, IPSec VPN |  |
| 27. | Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| 28. | Serwisy i licencje - w ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 3 lat. |  |
| 29. | Gwarancja oraz wsparcie - System powinien być objęty serwisem gwarancyjnym producenta przez okres min. 2 lat, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. |  |

**4.4. UPS 3500VA do podtrzymana urządzeń – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Obudowa | 1. Urządzenie UPS musi być wykonane w architekturze modułowej, z możliwością instalacji wolnostojącej (tzw. floor-stand) oraz w wersji do montażu w szafie przemysłowej rack zaoferowanej w tym postępowaniu2. Urządzenie musi być wyposażone we wszystkie elementy niezbedne do wykonania montazu j.w. – prowadnice i zestawy uchwytów, kable zasilające i dystrybutory zasilania do chronionych urządzeń (listwy PDU, rozgałęziacze, kabel logiczne dla komunikacji z modułami zarządzającymi)3. Urządzenie UPS musi posiadać wyprowadzone na front obudowy panel operatora wyposażony w przyciski sterujące i diody sygnalizacyjne lub w wyświetlacz dotykowy LCD – dla wykonywania wybranych czynności adminstratorskich (np. konfiguracja wybranych ustawień) oraz do sygnalizacji stanu pracy/awarii urządzenia UPS4. Urządzenie UPS musi posiadać wyprowadzone na tylnym panelu modułu głownego sekcje gniazd elektrycznych pozwalających na bezpośrednie podłączenie chronionych urządzeń (bez korzystania z listw PDU) w ilościach:- minimum 1 gniazdo standardu IEC320 16A- minimum 8 gniazd standardu IEC320 10A5. Urządzenie UPS musi obsługiwać 3 grupy/sekcje gniazd elektrycznych w celu:a) obsługi priorytetów podtrzymania zasilania dla wybranych urządzeń tj. kolejności wyłączania zasilania dla urządzeń o niższej krytyczności celem zapewnienia jak najdłuższego czasu podtrzymania zasilania dla urządzeń o najwyższym priorytecieb) możliwości cyklu wyłączenia-włączenia zasilania dla wybranej grupy urządzeń bez konieczności restartu/wyłączania całego urządzenia UPS6. Urządzenie UPS musi posiadać zabezpieczenie nadmiarowe (bezpiecznik) dla linii zasilającej UPS7. Urządzenie musi posiadać zainstalowany moduł zdalnego zarządzania poprzez protokół SNMP, z wyprowadzonym interfejsem Ethernet RJ-45 dla komunikacji poprzez sieć LAN8. Dostarczone rozwiązanie UPS nie może więcej niż 4U przestrzeni instalacyjne w szafie rack 19”9. Urządzenie UPS musi wspierać mechanizmy hot-plug dla wymiany online zespołow baterii w module głównym10. Urządzenie musi posiadać minimum 1 interfejs USB dla wykonywania operacji aktualizacji oprogramowania wewnetrznego  |  |
| 2 | Moc znamionowa | 1. Urządzenie UPS musi pozwalać na zabezpieczenie podtrzymania zasilania elektrycznego dla urządzeń informatycznych o łącznym poborze mocy minimum 3kVA przy zasilaniu 1-fazowym napięciem zmiennym w zakresie 220-240 VAC 50/60 Hz, 2. Urządzenie UPS musi bazować na technologii automatycznej regulacji napięcia zasilającego (AVR) lub na pełnej konwersji napięcia zasilającego3. Urządzenie UPS musi pozwalać na podłączanie minimum 8 zewnętrznych modułów bateryjnych w celu zwiększenia czasu podtrzmania zasilania dla chronionych urządzeń 4. Urządzenie UPS musi zapewniać podtrzymanie zasilania dla wszystkich chronionych urządzeń przez minimum 5 minut, przy podłączeniu takiej liczby zasilaczy na każdym chronionym urządzeniu aby zapewnić ich bezprzerwową pracę w przypadku całkowitej awarii zasilania zewnętrznego5. Typ zastosowanego urządzenie UPS musi pozwalać na zmianę sposobu zasilania z sieci zewnętrznej na zasilanie trójfazowym napięciem przemiennym 380V AC 50/60Hz bez konieczności wymiany modułów baterii lub samego modułu bazowego urządzenia UPS  |  |
| 3 | Inne funkcjonalności | 1. Z urządzeniem UPS należy dostarczyć oprogramowanie zarządzające przeznaczone do instalacji na platformach systemowych: MS Windows Server 2008R2/2012/2012R2, Vmware, SuSE Linux Enterprise Server, RedHat Enterprise Linux, Cirix XenServer2. Oprogramowanie musi zapewniać komunikację z wykorzystaniem interfejsu graficznego z bezpiecznym logowaniem Użytkownika3. Urządzenie musi obsługiwać tryb restartu przy braku zespołów baterii  |  |
| 4 | Gwarancja i serwis | 1. Całe rozwiązanie musi być objęte minimum 2-letnim okresem gwarancji z naprawą w miejscu instalacji urządzenia 2. Wraz z urządzeniem należy zapewnić subskrypcję na bezpłatną aktualizację (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania zarządzającego UPS-em3. Urządzenie UPS musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia urządzeń odnawianych, demonstracyjnych lub powystawowych4. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia  |  |

**4.5. Klimatyzacja redundantna min. 3,5kW - 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Moc | Moc (min. 3,5kW) wystarczająca do zapewniania poprawnej pracy serwerowni w skrajnie wysokich temperaturach zewnętrznych, przy pracującym UPS i sprzęcie serwerowo – macierzowym |  |
| 2. | Tryb użytkowania | Klimatyzator fabrycznie gotowy do pracy całorocznej, przy skrajnie niskich temperaturach występujących w zimie. |  |
| 3. | Odprowadzenie skroplin | Do instalacji ściekowej. Instalacja ma być przystosowana do pracy w skrajnie niskich temperaturach występujących w zimie. |  |
| 4. | Gwarancja | min. 24 miesięce |  |

Klimatyzację należy zainstalować i uruchomić w pomieszczeniu serwerowni wskazanym przez Zamawiającego.

**Środowisko serwerowo – macierzowe – 1 komplet**

**4.6. Serwer produkcyjny – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Obudowa | -Typu Rack, wysokość maksymalna 1U;-Dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack; |  |
| 2. | Płyta główna | -Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów dwunastordzeniowych;-Sumarycznie minimum 4 złącza PCI Express generacji 3 low profile, w tym minimum 2 złącza o prędkości x16 i 2 złącza o prędkości x8;-Zainstalowana dedykowana, wewnętrzna pamięci flash przeznaczonej dla wirtualizatora o pojemności 8 GB (niezależne od dysków twardych); |  |
| 3. | Procesory | -Zainstalowany jeden procesor 8-rdzeniowy w architekturze x86 osiągające w oferowanym serwerze w testach wydajności <https://www.cpubenchmark.net/cpu_list.php> min. 11000 pkt;-Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowane procesory, protokół poświadczony przez producenta serwera; |  |
| 4. | Pamięć RAM | -Zainstalowane min. 64 GB pamięci RAM typu DDR4 Registered, 2400Mhz w kościach o pojemności max. 16 GB-Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;- min. 12 gniazd pamięci RAM na płycie głównej, obsługa pamięci RAM DDR4-2400; |  |
| 5. | Kontrolery dyskowe, I/O | -Zainstalowany kontroler RAID min. 0, 1 6GBit/s |  |
| 6. | Dyski twarde | -Brak dysków;-Minimum 4 wnęki dla dysków twardych Hotplug 3,5;  |  |
| 7. | Kontrolery LAN | -Karta LAN wyposażona minimum w interfejsy: 4x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot i teamingu, RJ-45; |  |
| 8. | Kontrolery I/O | -zainstalowana karta HBA SAS  |  |
| 9. | Porty | -zintegrowana karta graficzna ze złączem VGA;- min. 5x USB, w tym minimum 2x USB 3.0 na panelu przednim, minimum 2x USB 3.0 dostępne z tyłu, 1x USB 3.0 dostępne wewnątrz; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;-możliwość rozbudowy serwera o złącze 1x RS-232-C; |  |
| 10. | Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o sprawności 94% o mocy maksymalnej 450W – sztuk 2-Redundantne wentylatory hotplug;  |  |
| 11. | Zarządzanie | -Wbudowane diody informujące o stanie serwera;-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
* Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
* Dostęp poprzez przeglądarkę Web (także SSL, SSH)
* Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
* Zarządzanie alarmami (zdarzenia poprzez SNMP)
* Możliwość przejęcia konsoli tekstowej
* Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
 |  |
| 12. | Oprogramowanie | Serwer należy dostarczyć z licencją VMW Essentials Kit z trzyletnim wsparciem; |  |
| 13. | Wspierane OS | -Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL |  |
| 14. | Gwarancja | -min. 2 lata gwarancji producenta serwera w trybie onsite z czasem reakcji w następnym dniu roboczym od zgłoszenia usterki;-Dostępność części zamiennych przez min. 5 lat od momentu zakupu serwera;-Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; |  |
| 15. | Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do postępowania sprzęt spełnia ten wymóg;-Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;-Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; |  |

**4.7. Macierz dyskowa – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1.  | Obudowa  | 1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe macierzy bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie.4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia)5) Obudowa powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy.  |  |
| 2.  | Pojemność  | 1) Model oferowanej macierzy musi obsługiwać min. 96 dysków 2,5” wykonanych w technologii hot-plug, także w konfiguracji z jednym kontrolerem w macierzy 2) Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie surowym (tzw. RAW) minimum 288TB bez konieczności wymiany zainstalowanych kontrolerów – wymagana zgodność z zapisami w aktualnej na moment składania oferty specyfikacji technicznej macierzy udostępnionej publicznie na stronie internetowej producenta lub jego przedstawiciela w Polsce.3) Model oferowanej macierzy musi umożliwiać rozbudowę do wyższego modelu z tej samej rodziny urządzeń w trybie w „data-in-place” tj. z wykorzystaniem wszystkich modułów półek rozszerzeń dyskowych wykorzystywanych przed rozbudową i z dostępem do wcześniej zapisanych danych.4) Macierz musi zawierać min. 12 dysków 2,5”SAS min. 600GB o prędkości obrotowej min. 10k. |  |
| 3.  | Kontrolery  | 1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami2) Każdy z kontrolerów macierzy musi posiadać po minimum 2GB pamięci podręcznej Cache – zawartość pamięci Cache z danymi do zapisu na dyskach musi być identyczna (tzw. cache mirror) dla wszystkich kontrolerów macierzy3) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik nie wymagający korzystania z podtrzymania jego zasilania – tj. bez zasilania zewnętrznego lub bateryjnego.5) Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia – wymaganie w przypadku konfiguracji z min. 2 kontrolerami.6) Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach w przypadku awarii macierzy z jednym zainstalowanym kontrolerem7) Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 1 interfejs RJ-45 Ethernet obsługujący połączenia z prędkością 100Mb/s i 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.8) Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC, iSCSI, SAS9) Macierz musi być wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych. |  |
| 4.  | Interfejsy  | 1) Oferowana macierz musi mieć minimum 2 porty SAS 6Gb/s, do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, wyprowadzone na każdy kontroler RAID. |  |
| 5.  | Poziomy RAID  | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: min. 0, 1 ,1+0, 5 , 50, 6  |  |
| 6.  | Wspierane dyski  | 1) wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex2) Oferowana macierz musi wspierać dyski hot-plug:- dyski mechaniczne HDD SAS o pojemności min. 300GB i prędkości obrotowej 15k rpm- dyski mechaniczne HDD SAS o pojemności min. 300GB i prędkości obrotowej 10k rpm, - dyski mechaniczne HDD NLSAS o pojemności min. 1TB i prędkości obrotowej min. 7,2k krpm,3) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”4) Macierz musi wspierać mieszaną konfigurację dysków SAS, NearLine-SAS w obrębie każdego pojedynczego modułu obudowy pozwalającego na instalacje dysków hot-plug.5) Macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych w trybie ręcznym i automatycznym z wykorzystaniem mechanizmu typu ‘time scheduler’ czyli w zadanym i/lub powtarzalnym oknie czasowym.8) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:- hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID- hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID. 9) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess) |  |
| 7.  | Opcje software’owe  | 1) Macierz musi umożliwiać zdefiniowanie min. 1024 woluminów (LUN) 2) Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 128 ścieżek logicznych.3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID i dysków bez konieczności wyłączania macierzy i bez konieczności wyłączania ścieżek logicznych dla podłączonych stacji/serwerów3) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupe dyskową5) Macierz musi posiadac wsparcie dla systemów operacyjnych : MS Windows Server 2008/2012, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, HP-UNIX, IBM AIX, SUN Solaris, VMWare , Citrix XEN Server6) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.7) Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności min. 128TB. 8) Macierz musi obsługiwać mechanizmy ograniczania wielkości pamięci podręcznej cache do obsługi wybranych woluminów LUN (tzw. cache partitioning) - jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ja wraz z macierzą w wariancie dla maksymalnej pojemności dyskowej danej macierzy oraz dla maksymalnej ilości obsługiwanych woluminów.9) Macierz musi umożliwiać rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD.10) Macierz musi obsługiwać migrację danych off-line z innych macierzy z wykorzystaniem minimum portów FC i bez wykorzystywania zewnętrznych serwerów w procesie kopiowania migrowanych danych 11) Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VASA, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji12) Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Off-loaded Data Transfer i Space Reclamation w środowiskach MS Windows 201213) Macierz musi obsługiwać mechanizmy Thin Provisioning czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.  |  |
| 8.  | Konfiguracja, zarządzanie  | 1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS).2) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 3) Musi być możliwe zdalne zarządzanie macierzą bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora4) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI  |  |
| 9.  | Gwarancja i serwis  | 1) Całe rozwiązanie musi być objęte minimum 24 miesięcznym okresem gwarancji z reakcją miejscu instalacji urządzenia w ciągu następnego dnia od zgłoszenia usterki 2) Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, w ciągu 36 miesięcy od daty zakupu. 3) Wraz z macierzą należy zapewnić subskrypcję na bezpłatną aktualizację (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego macierzy w całym okresie obowiązywania gwarancji 4) System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez protokół SNMP (wersja: 1 ,2c, 3) lub SMTP5) Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych 6) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia  |  |
| 10 | Inne | Wraz z macierzą należy dostarczyć 4 kable SAS (MiniSAS - miniSAS HD) o długości min. 3.0m |  |

**4.8.Urządzenie do wykonywania kopii zapasowej – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1. | Obudowa | -Typu Tower; 4U;-Obudowa musi być przekonwertowana do rack jedynie poprzez dodanie elementów fabrycznych producenta serwera (np. szyny rack czy tzw. „conversion-kit”;-Maksymalna wysokość serwera po konwersji do rack - 4U; |  |
| 2. | Płyta główna | -Wyprodukowana i zaprojektowana przez producenta serwera;-Minimum 4 złącza PCI Express w tym minimum 2 złącza PCI Express 3.0 x8 (prędkość i typ złącza);-Możliwość konwersji jednego ze złącz do złącza PCI 32bit-Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych);-Możliwość instalacji układ TPM 1.2; |  |
| 3. | Procesory | -Zainstalowany procesor 4-rdzeniowy w architekturze x86 osiągający w oferowanym serwerze w testach wydajności SPECint\_rate2006 min. 200 pkt;-Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowany procesor, protokół poświadczony przez producenta serwera; |  |
| 4. | Pamięć RAM | -Zainstalowane min. 32 GB pamięci RAM DDR4 2133Mhz w kościach o pojemności max. 16 GB-Wsparcie dla technologii zabezpieczania pamięci ECC;-Minimum 4 gniazda pamięci RAM, obsługa minimum 64GB pamięci RAM; |  |
| 5. | Kontrolery dyskowe, I/O | -Zainstalowany kontroler SAS 3.0 RAID min. 0, 1, 10, 5, 50, 6, 60 Cache 1 GB -Oferowany model serwera musi umożliwiać opcjonalną instalację wewnętrznego napędu LTO SAS zamiast napędu optycznego) |  |
| 6. | Dyski twarde | -Zainstalowane 2 dyski SATA o pojemności min. 200 GB Write-Intensive 3,5”, dyski Hotplug oraz 6 dysków SATA o pojemności min. 2 TB każdy,7,2K RPM 3,5”, dyski Hotplug-Minimum 8 wnęk dla dysków twardych Hotplug 3,5” w dostarczonej konfiguracji; -Możliwość rozbudowy serwera do obsługi co najmniej 12 dysków twardych Hotplug 3,5” |  |
| 7. | Inne napędy zintegrowane | -Zintegrowany naped DVD-RW-Zainstalowany wewnętrzny napęd LTO4 dostarczony warz z 5 taśmami LTO-4 oraz jedna taśmą czyszczącą; |  |
| 8. | Kontrolery LAN | - min. 2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot, RJ-45; |  |
| 9. | Kontrolery I/O | - zainstalowany kontroler SAS do obsługi napędu LTO  |  |
| 10. | Porty | -zintegrowana karta graficzna ze złączem VGA;- min. 9x USB, w tym minimum 5 złącz w standardzie USB 3.0 (2 na panelu przednim i 2 na panelu tylnym, 1 złącze wewnętrzne);-1x RS-232; |  |
| 11. | Zasilanie | -Zasilacz hotplug o sprawności 94% o mocy maksymalnej 450W; - Zainstalowany w miejsce drugiego zasilacza moduł umożliwiający potrzymanie serwera w razie awarii zasilania o mocy min. 380 W 12V |  |
| 12. | Zarządzanie | -Wbudowane diody informacyjne informujące o stanie serwera – minimum sygnalizacja (poprawna praca/usterka) dla komponentów jak: procesor, wentylatory, dyski twarde, temperatura wewnątrz obudowy, pamięci, zasilaczy; sygnalizacja pracy (zasilania), sygnalizacja identyfikacji (włączana zdalnie)-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
* Dedykowana karta LAN 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
* Dostęp poprzez przeglądarkę Web (także SSL, SSH)
* Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
* Zarządzanie alarmami (zdarzenia poprzez SNMP)
* Możliwość przejęcia konsoli tekstowej
* Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
 |  |
| 13. | Oprogramowanie | - Serwer należy dostarczyć z Windows Server 2012 R2 Standard lub równoważnym  |  |
| 14. | Oprogramowanie backupu | Serwer należy dostarczyć z odpowiednią ilością licencji oprogramowania do wykonywania kopii zapasowej środowiska wirtualnego Veeam Backup Essentials Standard |  |
| 15. | Wspierane OS | -Windows 2012 R2 Hyper-V, VMWare, Suse SLES11, RHEL 6 |  |
| 16. | Gwarancja | -min. 2 lata gwarancji onsite z reakcją w ciągu następnego dnia roboczego od zgłoszenia usterki.-Dostępność części zamiennych przez min. 5 lat od momentu zakupu serwera; |  |
| 17. | Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne lub oświadczenie producenta serwera;-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;-Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;-Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera jak również za pomocą software do zarządzania środowiskiem serwerowym dostarczonym razem z serwerem; |  |

**4.9. Oprogramowanie systemowe – 1 komplet**

System Operacyjny Microsoft Windows Server 2016 Standard lub równoważny – 3 szt.

Licencje dostępowe CAL na urządzenia – 30 szt.

**4.10. Access Point do budowy sieci WiFi – 8 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Rodzaj obudowy | Pokojowa |  |
| 2 | RAM | min. 1 GB |  |
| 3 | Pamięć fleszowa | min. 256 MB |  |
| 4 | Protokół komunikacyjny danych | IEEE 802.11b,IEEE 802.11a,IEEE 802.11g,IEEE 802.11n,IEEE 802.11ac (draft 5.0) |  |
| 5 | Pasmo częstotliwości | 2.4 GHz,5 GHz |  |
| 6 | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 7 | Zasilanie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 8 | Wymiary (szer./głęb./wys.) | max. 21.08 cm x 21.08 cm x 50.8 cm |  |
| 9 | Waga | max. 1.41 kg |  |
| 10 | Antena | Wewnętrzna |  |
| 11 | Kierunkowość | Antena dookólna |  |
| 12 | Poziom uzyskany | min. 5 dBi |  |
| 13 | Interfejsy | 1 x 1000Base-T (PoE+) - RJ-45  |  |
| 1 x konsola - RJ-45  |  |
| 1 x USB 2.0 - Type A |  |
| 14 | Obsługuje Power Over Ethernet (PoE) | PoE+ |  |
| 15 | Zasilacz | Adapter mocy zewnętrznej |  |
| 16 | Wymagane napięcie | AC 120/230 V ( 50 - 60 Hz ) |  |
| 17 | Zużycie energii w trybie aktywności | max. 16 wat |  |
| 18 | Wymaganie dodatkowe | w celu wspólnego zarządzania, tego samego producenta co przełącznik |  |
| 19 | Gwarancja | min. 24 miesięce on site NBD |  |

**4.11. Siec LAN – 1 komplet**

W pomieszczeniach budynków należących do Zamawiającego należy wykonać okablowanie do Access Pointów.

Okablowanie należy wykonać kablami kat min. 6 z punktu dystrybucyjnego do Access Pointa. Należy skonfigurować Access Pointy tak aby urządzenia podłączone do nich mogły w bezpieczny sposób korzystać z zasobów serwerowni oraz Internetu.

Dodatkowo w budynku w Prabutach należy wykonać sieć LAN składającą się z 24 punktów PEL na poziomie -1. Przez PEL należy rozumieć punkt elektryczno-logiczny składający się z 2xRJ45+2xDATA. Należy zastosować kabel min. 6 kategorii.

Urządzenia we wszystkich lokalizacjach muszą być tak skonfigurowane aby została stworzona jedna sieć z dostępem do serwerów będących w lokalizacji w Prabutach, sieć ma być wykonana w taki sposób aby można było podłączyć sprzęt komputerowy użytkowników dostarczony w ramach tego postępowania do zasobów serwerowni i Internetu.

Dostarczone szafy należy zamontować w miejscach wskazanych przez Zamawiającego i wyposażyć w zakupiony w tym postępowaniu sprzęt.

**5. Komputer typu AiO – 30 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
|  | Typ: | Komputer typu AiO |  |
| 1. | Ekran | Przekątna: min 21,5 calaRozdzielczość: min. FHD 1080p (1920x1080), podświetlenie LED, jasność min. 200 cd/m2, format 16:9, kontrast min. 1000:1, matryca matowa |  |
| 2. | Obudowa | Zintegrowana z monitorem (AIO)Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) Założona blokada kensington musi uniemożliwiać otworzenie tylnej obudowyPodstawa musi umożliwiać regulację kąta nachylenia w zakresie co najmniej –5° do przodu oraz 45° do tyłuMożliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego z możliwością demontażu stopy. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnymCzytnik kart multimedialnych min. 3 in 1 |  |
| 3. | Płyta główna | Wyprodukowana przez producenta komputera |  |
| 4. | Procesor | Procesor klasy x86, min. 4 rdzeniowy, taktowany zegarem co najmniej 2,7 GHz, pamięcią cache CPU co najmniej 6 MB zapewniający wydajność CPU mierzoną przez PassMark Software na poziomie min. 6 400 pkt wynik dostepny na stronie <http://www.cpubenchmark.net/> |  |
| 5. | Pamięć operacyjna | min. 8GB DDR4 2133MHz z możliwością rozszerzenia do 32 GB Ilość banków pamięci: min. 2 szt.Ilość wolnych banków pamięci: min. 1 szt. |  |
| 6. | Dysk twardy | min. 250GB SSD SATA, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |  |
| 7. | Napęd optyczny | Nagrywarka DVD +/-RW wraz z dołączonym oprogramowaniem do odtwarzania i nagrywania |  |
| 8. | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki Obsługująca funkcje min.:DirectX 12,OpenGL 4.4 |  |
| 9. | Audio/Video | Wbudowane głośniki stereo 2 x 2W, wbudowany mikrofon, wbudowana kamera min. HD720p z wbudowaną mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery |  |
| 10. | Karty sieciowe | 10/100/1000 – złącze RJ45 WiFi ac/b/g/n + BT 4.0  |  |
| 11. | Porty/złącza | Wbudowane (minimum): DisplayPort, 6 x USB z czego min 2 x USB3.0 z boku obudowy, czytnik kart multimedialnych min. 3-w-1, 1 x RJ 45 (LAN), 1 x wyjście na słuchawki i mikrofon (Combo). Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |  |
| 12. | Klawiatura/mysz | Klawiatura przewodowa w układzie US USB. Mysz przewodowa optyczna (scroll) USB |  |
| 13. | Zasilacz | Maksymalna moc zasilacza nie większa niż 150W 85% sprawności |  |
| 14. | System operacyjny | Microsoft Windows 10 Professional PL 64bit lub równoważne |  |
| 15. | BIOS | -  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, producencie komputera- numerze seryjnym,- zainstalowanym procesorze, jego taktowaniu i ilości rdzeni- ilości pamięci RAM wraz z taktowaniem,- napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego)Możliwość z poziomu Bios:- wyłączenia wbudowanej kamery, karty WiFi, karty audio, czytnika kart, mikrofonu, bocznych przycisków zlokalizowanych na obudowie- ustawienia hasła: administratora, Power-On, - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan)- obsługa Bios za pomocą klawiatury i myszy |  |
| 16. | Certyfikaty i standardy | Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty).ENERGY STAR Deklaracja zgodności CE (załączyć do oferty).Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. |  |
| 17. | Waga/rozmiary urządzenia | Waga urządzenia wraz ze stopą max. 8 kgSuma wymiarów (bez podstawy) nie może przekraczać 1000 mm. Suma wymiarów z podstawą nie może przekraczać 1300 mm. |  |
| 18. | Gwarancja | min. 2 lata świadczona w miejscu użytkowania sprzętu (on-site) w następnym dniu roboczymOświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |  |

**6. Drukarka monochromatyczna A4 – 10 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Technologia druku | Monochromatyczna laserowa lub LED |  |
| 2 | Szybkość drukowania w A4 | min. 40 str./min w mono |  |
| 3 | Czas pierwszego wydruku  | do 7 sekund |  |
| 4 | Rozdzielczość rzeczywista | min. 1200 x 1200 dpi |  |
| 5 | Pamięć (RAM)  | min. 512 MB  |  |
| 6 |  Szybkość procesora  | min. 650 MHz |  |
| 7 | Obciążenie | Maksymalne obciążenie do 80 000 stron miesięcznie |  |
| 8 | Języki druku  | PCL5e, PCL6, PDF (v1.7), PostScript 3 emulacja |  |
| 9 | Zespół drukowania  | Dupleks mechaniczny |  |
| 10 | Złącza  | Port USB 2.0, Ethernet 10/100/1000BaseTX, Urządzenie musi posiadać możliwość instalacji karty sieciowej bezprzewodowej WLAN802.11a/b/g/n |  |
| 11 | Kompatybilność z systemami operacyjnymi  | Windows 7 (32-bitowy i 64-bitowy), Windows 8 (32-bitowy i 64-bitowy), Windows 8.1 (32-bitowy i 64-bitowy)indows Server 2003 (32-bitowy i 64-bitowy), Windows Vista ( 32-bitowy i 64-bitowy), Windows Server 2008 (32-bitowy i 64-bitowy), Windows Server 2008 R2 (64-bitowy), Windows Server 2012 (64-bitowy), Windows Server 2012 R2 (wersja 32-bitowa i 64-bitowa); Linux PPD; Mac OS 10.6.8-10.7, 10.8 , 10,9 |  |
| 12 | Pojemność papieru  | Podajnik na min. 250 arkuszy 80 g/m2;Podajnik uniwersalny: min. 100 arkuszy 80 g/m2 |  |
| 13 | Format papieru  |  A4, A5, B5, A6 |  |
| 14 | Gramatura papieru  | min. 60 – 163 g/m2 |  |
| 15 | Gwarancja | 24 miesięce, naprawa w ciągu 24 h w miejscu instalacji lub sprzęt zastępczy. |  |
| 16 | Wymagane dokumenty: | Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu Certyfikat ISO 14001:2004 producenta oferowanego sprzętu  |  |
| 17 |  Materiały eksploatacyjne: | Wymagana rozdzielność bębna i tonera. Toner startowy na min. 2 tys. stron zgodnie z normą ISO/ISC 19752Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami) umożliwiającym wydruk przynajmniej 7 000 stron A4 przy pokryciu zgodnie z normą ISO/ISC 19752. Toner musi być tego samego producenta co drukarka, nie mogą być regenerowane. |  |

**7. Urządzenie wielofunkcyjne monochromatyczne A4 – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Drukowanie: | Szybkość drukowania: min. 33 str./minSzybkość druku dwustronnego: min. 18 str/minCzas pierwszego wydruku: max. 6,5 sekundRozdzielczość: min. 1200 x 1200 dpiJęzyki druku: min. PCL5e, PCL6, IBM-PPR, Epxon-FX,XPSZespół drukowania: Dupleks mechaniczny |  |
| 2 | Skanowanie: | Rozdzielczość skanowania: min. 600 x 600 dpiMaksymalna szybkość skanowania: Do 6 s/stronę w kolorze, do 2s/stronę w czerniGłębia kolorów: Wejście min. 48 bit/Wyjście 24 bitPodawanie dokumentów: Automatyczny podajnik dokumentów wraz z duplexem na min. 50 arkuszy, skaner płaskiFormat M-TIFF, PDF, XPS, JPEG, GIF, PNGKsiążka adresowa: LDAP, min. 300 adresów e-mail, min. 20 grup adresowychSkanowanie do: FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB, |  |
| 3 | Kopiowanie: | Czas wykonania pierwszej kopii: max.10 sekundSzybkość kopiowania: do 33 kopii/minRozdzielczość kopiowania: do 600 x 600dpiZmniejszanie/powiększanie: Zoom min. 25-400%Maksymalna liczba kopii: 99 |  |
| 4 | Faksowanie: | Złącza: RJ11 x 2 (Line/Tel), PSTN, Linia PBXSzybkość: ITU-T G3(Super G3) do 33,6kbps, do 2 s/str.Szybkie wybieranie: min. 16 przycisków szybkiego wybierania, min. 300 numerówLista rozgłaszania: Maksimum 100Pamięć stron: min. 4MB |  |
| 5 | Interfejs i oprogramowanie: | Złącza: Port USB 2.0, Ethernet 10/100/1000BaseTXKomunikacja bezprzewodowa: Tak, moduł bezprzewodowej karty sieciowej wbudowanej w urządzenie.Kompatybilność z systemami operacyjnymi: Windows XP (32-bit & 64-bit) / Server 2003 (32-bit & 64-bit) / Server 2008 (32-bit & 64-bit) / Server 2008 R2 (64-bit) / Vista (32-bit & 64-bit) / 7 (32-bit & 64-bit); Linux PPD, Mac OS X 10.6.8 - 10.7, 10.8, 10.9Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje:* funkcjonować w środowisku Windows;
* obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT)
* podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki;
* podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku;
* możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek;
* podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów);
* możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.
 |  |
| 6 | Podawanie papieru: | Pojemność papieru:* Podajnik 1: min. 250 arkuszy 80 g/m2;
* Podajnik uniwersalny: min. 100 arkuszy 80 g/m2;
* Możliwość instalacji dodatkowego podajnika papieru o pojemności min. 530 arkuszy 80g/m2

Format papieru:* Podajnik 1: A4, A5, B5, A6
* Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6,
* Druk dwustronny: A4, B5

Gramatura papieru:* Podajnik 1: min. 60 – 120 g/m2;
* Druk dwustronny: min. 60 – 120 g/m2;
* Podajnik uniwersalny: min. 60 – 120 g/m2
* Podajnik skanera: min. 60 – 105 g/m2

Odbiornik papieru: Do 150 arkuszy stroną zadrukowaną do dołu |  |
| 7 | Pozostałe parametry techniczne: | Pamięć (RAM): Standardowa pamięć RAM: min. 512 MB Obciążenie: Maksymalne obciążenie do 60 000 stron miesięcznie |  |
| 8 | Gwarancja: | min. 2 lata gwarancji producenta drukarki - naprawa w miejscu instalacji w ciągu 24h od daty zgłoszenia lub sprzęt zastępczy. |  |
| 9 | Wymagane dokumenty: | Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu - dokumenty potwierdzające załączyć do oferty. Certyfikat ISO 140001:2004 producenta oferowanego sprzętu - dokumenty potwierdzające załączyć do oferty. |  |
| 10 | Materiały eksploatacyjne: | Wymagana rozdzielność bębna i tonera. Toner startowy na min. 2 tys. stron zgodnie z normą ISO/ISC 19752Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami) umożliwiającym wydruk przynajmniej 7 000 stron A4 przy pokryciu zgodnie z normą ISO/ISC 19752. Toner musi być tego samego producenta co drukarka, nie mogą być regenerowane. |  |

**8. Tablet – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Wyświetlacz | min. 10,1 cala TFTmin. 16 777 216 kolorów, min. 1920 x 1200 pikseli |  |
| 2 | Pamięć | RAM: min. 3 GBPamięć typu flash: do 16 GBGniazdo rozszerzeń: karty microSD™, do 64 GB |  |
| 3 | Procesor  | Czterordzeniowy procesor o częstotliwości min. 2,3 GHz |  |
| 4 | Aparat | min. 8,1 Megapikselamin. 8-krotne powiększenie cyfroweAparat na przednim panelu min. (2,2 MP, 1080p) |  |
| 5 | Wytrzymałość | Wodoodporność (IP55 i IP58)Odporność na kurz (IP55) |  |
| 6 | System operacyjny | Android min. 6.0 |  |
| 7 | Waga | max. 450g |  |
| 8 | Gwarancja | min. 24 miesięce |  |

**9. System antywirusowy – 40 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Program | Ochrona przed spyware oraz adware, ochrona przed wirusami, trojanami, robakami, skanowanie poczty, ruchu internetowego, plików w czasie rzeczywistym. W tym ochrona min 3 serwerów. System musi posiadać moduł centralnego zarządzania. System należy zainstalować na komputerach/laptopa i serwerach zakupionych w ramach tego samego postępowania.Możliwość aktualizowania bazy wirusów przez okres 60 miesięcy. |  |

**10. Oprogramowanie biurowe (np. Microsoft Office) – 5 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
| 1 | Program | Zawierające aplikacje: Edytor tekstu służący do tworzenia dokumentów tekstowych, które mogą zawierać tabele, wykresy, rysunki, równania, oraz inne obiekty występujące w środowisku Windows. Arkusz kalkulacyjny, którego głównym zastosowaniem powinno być dokonywanie obliczeń zestawionych w formie tabelarycznej. Możliwość stosowania licznych funkcji matematycznych, finansowych i bazodanowych dostępnych w programie. Możliwość półautomatycznego powielania tworzonych formuł z zastosowaniem różnych wariantów adresowania (adresowanie względne, adresowanie bezwzględne, adresowanie mieszane). Program służący do tworzenia wielu typów wykresów, przydatnych między innymi w fizyce, matematyce i ekonomii. Zawierający też system zestawiania raportów z użyciem tzw. tabel przestawnych, wykorzystywany przy wykonywaniu analiz biznesowych. Program do tworzenia prezentacji multimedialnych, w którym można wstawiać i edytować klipy wideo, a także dodawać zanikanie i efekty formatowania, oznaczać sceny oraz przycinać klipy wideo w celu nadania prezentacji wyglądu profesjonalnego multimedium za pomocą narzędzi do edytowania obrazów (włącznie z narzędziami: wszechstronnych efektów artystycznych i zaawansowanej korekcji, koloru oraz przycinania) można dostosować każdy obraz w prezentacji tak, aby wyglądał jak najlepiej. Wersja polskojęzyczna.Oprogramowanie kompatybilne z systemem HIS w zakresie generowania raportów.  |  |

**11. Laptop – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa producenta i model (podać)** |  |
| **Minimalne wymagane parametry** | **Parametr oferowany** |
|  | Typ: | Komputer typu laptop |  |
| 1 | Wydajność obliczeniowa: | Procesor klasy x86, min. 2 rdzeniowy, taktowany zegarem co najmniej 2,2 GHz, z pamięcią cache CPU co najmniej 3 MB, powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 3500 punktów Passmark CPU Mark |  |
| 2 | Pamięć operacyjna: | min. 8GB 2133 MHz możliwość rozbudowy do max 16 GB, |  |
| 3 | Dysk twardy | Min. 240 GB SATA, SSD, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników. |  |
| 4 | Karta graficzna | Zintegrowana karta graficzna wykorzytująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki  |  |
| 5 | Karta dźwiękowa | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  |  |
| 6 | Karty sieciowe | 10/100/1000 – złącze RJ45 WiFi b/g/n/ac |  |
| 7 | System operacyjny | Microsoft Windows 10 Professional PL 64bit lub równoważne |  |
| 8 | Klawiatura | U układzie QWERTY, wydzielona klawiatura numeryczna. |  |
| 9 | Bateria | min 4-komorowa, min. 2200 mAh, Li-Ion |  |
| 10 | Ekran | 15’6”, matryca matowa, LED, rozdzielczość 1920 x 1080 |  |
| 11 | Waga | max. 2,3 kg z baterią |  |
| 12 | Porty | min. 3 USB, min. USB 3.0 – 2 szt, HDMI, VGA (D-sub), RJ-45, czytnik kart pamięci, wyjście słuchawkowe/wejście mikrofonu |  |
| 13 | Certyfikaty i standardy | Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty).Deklaracja zgodności CE (załączyć do oferty). |  |
| 14 | Gwarancja | 2 lata świadczona w miejscu użytkowania sprzętu (on-site) w następnym dniu roboczymOświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. |  |

……………………………………………………………… ………………………………………………………………………..

Miejscowość, data Podpis Wykonawcy