**Załącznik nr 3c do SIWZ**

# Opis przedmiotu zamówienia sprzęt komputerowy

Przedmiot zamówienia obejmuje dostawę zgodnie z poniższym wykazem:

| **1. Przełącznik LAN – 3 sztuki** | |
|---|---|
| **Lp.** | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |
| 1. | Minimum 48 portów 100BaseTX/1000BaseT ze wsparciem dla standardu 802.3at (PoE+) |
| 2. | Minimum jeden slot na moduły pozwalające na rozbudowę o dodatkowe porty 10Gb i 40Gb. W chwili składania oferty muszą być dostępne co najmniej moduły minimum 4 portowe 10Gb SFP+ oraz minimum 2 portowe 40Gb QSFP+. Moduły muszą być dostępne z przodu obudowy. Dopuszcza się większą liczbę modułów o mniejszej gęstości, pod warunkiem, że sumaryczna liczba dostępnych portów będzie nie mniejsza niż wymagana per moduł i wszystkie moduły dostępne będą z przodu obudowy. |
| 3. | Slot obsadzony modułem wyposażonym w 4 porty SFP+ |
| 4. | Przepustowość: minimum 320 Gb/s |
| 5. | Wydajność: minimum 190 Mp/s |
| 6. | Bufor pakietów: minimum 13 MB |
| 7. | Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych |
| 8. | Przełącznik musi umożliwiać instalację co najmniej 4 dedykowane porty umożliwiające łączenie w stos. Wydajność portów stackujących co najmniej 40 Gbps na port. Oprogramowanie przełącznika musi umożliwiać połączenie co najmniej 10 urządzeń w stos. Przełączniki połączone w stos z punktu widzenia reszty infrastruktury powinny być widoczne jako jedno urządzenie. Porty służące do połączenia w stos muszą być niezależne od minimalnej liczby wymaganych portów liniowych, nie mogą także ograniczać możliwości ich rozbudowy. |
| 9. | Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. |
| 10. | Budżet mocy PoE na pojedynczym zasilaczu nie mniejszy niż 370W |
| 11. | Modularne, redundantne wentylatory. Moduł wentylatorów musi mieć możliwość wymiany „na gorąco” (na działającym urządzeniu) |
| 12. | Wielkość tablicy routingu: minimum 10000 wpisów |
| 13. | Tablica adresów MAC o wielkości minimum 64000 pozycji |
| 14. | Obsługa Jumbo Frames |
| 15. | Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9) |
| 16. | Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN |
| 17. | Obsługa standardu IEEE 802.1v |
| 18. | Wsparcie dla VxLAN |
| 19. | Dostęp do urządzenia przez konsolę szeregową (RS-232 i USB), HTTPS, SSHv2 i SNMPv3 |
| 20. | Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) |
| 21. | Obsługa Secure FTP |
| 22. | Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP) |
| 23. | Obsługa dystrybuowanych łączy agregowanych LACP – łączy agregowanych wychodzących z dwóch, różnych, niezależnych i oddzielnie zarządzanych (nie połączonych w stos) przełączników |

| | |
|---|---|
| | (tzw. Multi-chassis Link Aggregation, MLAG, MC-LAG, Distributed Trunking) |
| 24. | Obsługa Simple Network Time Protocol (SNTP) v4 |
| 25. | Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping) |
| 26. | Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM, BGP |
| 27. | Obsługa 802.1ad (Q-in-Q) |
| 28. | Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) |
| 29. | Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED) |
| 30. | Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting |
| 31. | Obsługa uwierzytelniania użytkowników zgodna z 802.1x |
| 32. | Obsługa uwierzytelniania użytkowników w oparciu o lokalną bazę adresów MAC |
| 33. | Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS |
| 34. | Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW |
| 35. | Obsługa różnych metod uwierzytelniania (802.1x, MAC, WWW) w tym samym czasie na tym samym porcie |
| 36. | Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie |
| 37. | Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ |
| 38. | Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+ |
| 39. | Wbudowany serwer DHCP |
| 40. | Obsługa funkcji User Datagram Protocol (UDP) helper |
| 41. | Obsługa blokowania nieautoryzowanych serwerów DHCP |
| 42. | Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) |
| 43. | Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP |
| 44. | Obsługa protokołu OpenFlow w wersji co najmniej 1.0 i 1.3 |
| 45. | OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic |
| 46. | Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP) |
| 47. | Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow. |
| 48. | Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow. |
| 49. | Obsługa standardu 802.3az Energy Efficient Ethernet |
| 50. | Obsługa standardu 802.1AE MACsec |
| 51. | Zakres pracy od 0 do 45°C |
| 52. | Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 45 cm. |
| 53. | Dożywotnia (tak długo jak Zamawiający posiada produkt, minimum 10 lat) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR |

| | |
|---|---|
| | NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |

| **2. Firewall z analizatorem ruchu sieciowego – 1 sztuka** | | |
|---|---|---|
| **Nazwa składnika/parametru technicznego sprzętu** | | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |
| Architektura systemu ochrony | Typ systemu ochrony | • System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.<br>• Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge). |
| | Wymagania systemowe | • System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.<br>• Obsługa nielimitowanej ilości hostów w sieci chronionej.<br>• Typ procesora: Intel multi-core technology<br>• Pamięć RAM: nie mniej niż 8 GB<br>• Metalowa obudowa o wysokości maksymalnie 1U przeznaczona do montażu w szafie RACK.<br>• Minimalna liczba i typ interfejsów fizycznych: 6x GE (IEEE 1000Base-T), 2x GE (IEEE 1000Base-X), 2x USB 3.0 (Type-A), 1x Console (RJ-45 lub DB9) z możliwością rozbudowy o co najmniej 8 x GE (IEEE 1000Base-T lub IEEE1000Base-X).<br>• Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)<br>• Minimalna liczba nowych połączeń na sekundę: 135 000<br>• Minimalna liczba jednoczesnych połączeń: 8 000 000<br>• Minimalna przepustowość Firewall (IMIX): 5 500 Mbps<br>• Minimalna przepustowość IPS: 7 000 Mbps<br>• Minimalna przepustowość Web Proxy AV: 2 000 Mbps<br>• Minimalna przepustowość IPSec: 1 250 Mbps<br>• Minimalna liczba równoczesnych tuneli IPSec VPN: 1 300<br>• Minimalna liczba równoczesnych tuneli SSL VPN: 300<br>• Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB.<br>• Zintegrowany wielofunkcyjny wyświetlacz LCD. |
| Podstawowe funkcje systemu ochrony | Zarządzanie i utrzymanie | • Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).<br>• Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup.<br>• Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.<br>• Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości |

| | | |
|---|---|---|
| | | min. 4096 bitów.<br>• Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.<br>• System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.<br>• System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.<br>• System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.<br>• Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).<br>• System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.<br>• Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.<br>• System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.<br>• Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.<br>• System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.<br>• Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik).<br>• System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.<br>• System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on-premise lub on-cloud.<br>• Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z |

| | | |
|---|---|---|
| | | zapisem do pliku lokalnego, do serwera FTP lub via email.<br>• Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.<br>• Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.<br>• Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.<br>• Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.<br>• Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).<br>• System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.<br>• W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie). |
| | Zapora sieciowa, konfiguracja sieciowa oraz routing | • Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.<br>• Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.<br>• System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.<br>• Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.<br>• Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.<br>• System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN.<br>• Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.<br>• Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.<br>• System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).<br>• System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).<br>• System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).<br>• Rozwiązanie powinno zapewniać obsługę routingu statycznego. |

| | | |
|---|---|---|
| | | • Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).<br>• Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).<br>• System powinien oferować wsparcie dla IGMP snooping.<br>• Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy).<br>• Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.<br>• Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).<br>• System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.<br>• System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.<br>• Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.<br>• Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.<br>• Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.<br>• Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.<br>• Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).<br>• System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.<br>• System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania.<br>• Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). |
| | Podstawowe kształtowanie pasma oraz limity ilości danych | • System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.<br>• Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.<br>• System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. |
| | Bezpieczna sieć bezprzewodowa | • System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.<br>• Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge |

| | | |
|---|---|---|
| | | oraz Wireless Repeater.<br>• Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.<br>• Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.<br>• Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej.<br>• Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej.<br>• Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.<br>• Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication).<br>• Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition).<br>• System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.<br>• Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.<br>• System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden.<br>• System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe.<br>• Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection). |
| | Autoryzacja użytkowników | • Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.<br>• Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.<br>• System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+.<br>• Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.<br>• Dodatkowo system powinien umożliwiać autoryzację |

| | | |
|---|---|---|
| | | dwustopniową za pomocą hasła jednorazowego (One Time Password).<br>• Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.<br>• System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.<br>• Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.<br>• Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal. |
| | Samoobsługowy portal dla użytkowników | • Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.<br>• Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).<br>• Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.<br>• Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.<br>• Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.<br>• Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika.<br>• Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email. |
| | Podstawowe opcje VPN | • System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:<br>• Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)<br>• Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika). |
| | Klient IPSec VPN (dostępny osobno) | • Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.<br>• Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.<br>• Wsparcie dla split-tunneling.<br>• Wsparcie dla NAT-traversal.<br>• Monitorowanie stanu połączenia. |
| Ochrona sieci | IPS | • Moduł ochrony klasy IPS z bazą minimum 7000 sygnatur.<br>• Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.<br>• Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.<br>• Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur |

| | | |
|---|---|---|
| | | w celu zredukowania opóźnień w przesyłaniu pakietów.<br>• System powinien generować alerty w przypadku wykrycia ataku. |
| | ATP | • System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control. |
| | Clientless VPN | • Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5. |
| Ochrona i kontrola Web oraz aplikacji | Ochrona i kontrola Web | • Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.<br>• Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).<br>• System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.<br>• System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.<br>• Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups).<br>• Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch).<br>• Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.<br>• System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.<br>• System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.<br>• Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.<br>• System powinien zapewniać możliwość emulacji skryptów JavaScript.<br>• Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.<br>• Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.<br>• Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.<br>• Rozwiązanie powinno umożliwiać blokadę stron HTTPS.<br>• Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.<br>• Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.<br>• System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator |

| | | |
|---|---|---|
| | | powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji. |
| | Ochrona i kontrola aplikacji | • Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2500 aplikacji.<br>• Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.<br>• Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.<br>• Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.<br>• Rozwiązanie powinno umożliwiać blokowanie:<br>- aplikacji, które pozwalają na transfer plików (np. P2P).<br>- komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.<br>- proxy uruchamianych poprzez przeglądarki internetowe.<br>- streaming media (radio internetowe, Youtube, Vimeo).<br>• Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo. |
| | Kształtowanie pasma dla Web i Aplikacji | • Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie.<br>• Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.<br>• Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared). |
| Logowanie i raportowanie | Logowanie i raportowanie | • System musi umożliwiać składowanie oraz archiwizację logów za pomocą wbudowanego i bezpłatnego mechanizmu o cechach analizatora ruchu, posiadającego również funkcję integracji z zewnętrznym oprogramowaniem Producenta.<br>• System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.<br>• System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.<br>• System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.<br>• System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).<br>• Rozwiązanie powinno umożliwiać wysyłanie raportów via |

| | | |
|---|---|---|
| | | email.<br>• Rozwiązanie powinno generować raporty w PDF, HTML i XLS.<br>• Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.<br>• System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza<br>• System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację<br>• Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.<br>• System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.<br>• System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji. |
| Pozostałe | Certyfikaty | • CE, FCC Class A, CB, VCCI, C-Tick, UL, CCC |
| | Subskrypcje | • Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 5 lat. |
| | Gwarancja i wsparcie | • Wsparcie techniczne w trybie 24x7 na okres nie krótszy niż 5 lat. |

| **3. Serwer – 2 sztuki** | |
|---|---|
| **Nazwa składnika/parametru technicznego sprzętu** | **Minimalne wymagania w zakresie składników i parametrów technicznych sprzętu** |
| **Procesor** | Zainstalowane dwa procesory 10-rdzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 896 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org dla dwóch procesorów.<br>Wymagane jest złożenie wraz z ofertą wyników w/w testów. Wyniki powinny zostać przedstawione w postaci wydruku z pliku PDF oryginalnie pobranego ze strony spec.org. |
| **Pamięć operacyjna** | min. 256GB pamięci RAM DDR4 RDIMM 2667MT/s z korekcją błędów ECC, SDDC, memory mirror, memory sparing, lockstep. Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5TB pamięci RAM. |
| **Pamięć masowa** | Zainstalowane 2x120GB SSD SATA oraz 4x1.2TB SAS 12Gb/s 10k. Możliwość instalacji do 8 dysków 2.5” dysków SATA, SAS, SSD hot-plug.<br>Wbudowany napęd DVD-RW |
| **Interfejs sieciowy** | Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Możliwość instalacji wymiennie modułów udostępniających:<br>- dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.<br>- cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+.<br>- dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT.<br>- dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.<br>Zainstalowana dodatkowo jedna karta czteroportowa 1GbE w standardzie Base-T, dwie dwuportowe karty 10GbE w standardzie Base-T oraz karta dwuportowa FC |

| | |
|---|---|
| | 16Gb/s. |
| **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Sloty PCI Express** | Minimum 6 slotów PCI-Express generacji 3 o prędkości x8, Min. 2 sloty PCI-Express generacji 3 o prędkości x16 pełnej długości i wysokości |
| **Zasilanie i chłodzenie** | Minimum 2szt., redundantne, typu hot-plug o mocy maksymalnie 750W<br>Redundantne wentylatory |
| **Kontroler dyskowy** | Zainstalowany sprzętowy kontroler RAID zapewniający obsługę zabezpieczeń RAID na poziomie 0/1/10,5,50,6,60. Moduł nieulotnej pamięci cache minimum 2GB. Wsparcie dla dysków samoszyfujących. |
| **Grafika** | Zintegrowana z płytą główną umożliwiająca wyświetlanie obrazu w rozdzielczości min. 1920x1200 |
| **Dodatkowe interfejsy** | min. 3 porty USB 2.0, 2 porty USB 3.0 oraz 1 port Micro-usb, 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.<br>Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń. |
| **Gwarancja** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego.<br><br>W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.<br>Do oferty wymagane jest dołączenie oświadczenie producenta komputera, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej przejmie na siebie wszelkie zobowiązania związane z serwisem.<br><br>Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. |
| **Zarządzanie i obsługa techniczna** | Panel diagnostyczny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesorów, pamięciach, dyskach, wentylatorach, kontrolera RAID, kartach PCI-E, zasilaczach, temperaturze.<br><br>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:<br>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej<br>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera)<br>• szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika<br>• możliwość podmontowania zdalnych wirtualnych napędów |

| | |
|---|---|
| | • wirtualną konsolę z dostępem do myszy, klawiatury<br>• wsparcie dla IPv6<br>• wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH<br>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer<br>• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer<br>• integracja z Active Directory<br>• możliwość obsługi przez dwóch administratorów jednocześnie<br>• wsparcie dla dynamic DNS<br>• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej<br>• możliwość podłączenia lokalnego poprzez złącze RS-232<br>• możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.<br><br>Czytnik NFC umożliwiający zarządzanie serwerem poprzez aplikacje mobilną udostępnioną przez producenta serwera.<br><br>Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności min. 32GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.<br>Serwer musi posiadać deklaracja CE.<br>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2008 R2 x64, Microsoft Windows 2012, Microsoft Windows 2012R2 x64. |
| **Oprogramowanie** | Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:<br>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych<br>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta<br>• Wsparcie dla protokołów– WMI, SNMP, IPMI, , Linux SSH<br>• Możliwość oskryptowywania procesu wykrywania urządzeń<br>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram<br>• Szczegółowy opis wykrytych systemów oraz ich komponentów<br>• Możliwość eksportu raportu do CSV, HTML, XLS<br>• Grupowanie urządzeń w oparciu o kryteria użytkownika<br>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach<br>• Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń<br>• Szybki podgląd stanu środowiska<br>• Podsumowanie stanu dla każdego urządzenia<br>• Szczegółowy status urządzenia/elementu/komponentu<br>• Generowanie alertów przy zmianie stanu urządzenia<br>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń<br>• Integracja z service desk producenta dostarczonej platformy sprzętowej<br>• Możliwość przejęcia zdalnego pulpitu |

| | |
|---|---|
| | • Możliwość podmontowania wirtualnego napędu<br>• Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu<br>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów<br>• Możliwość importu plików MIB<br>• Przesyłanie alertów „as-is" do innych konsol firm trzecich<br>• Możliwość definiowania ról administratorów<br>• Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów<br>• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)<br>• Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta<br>• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów<br>▪ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych<br>▪ Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).<br>▪ Zainstalowana jedna karta flash o pojemności min. 32GB. |

| **4. Stacjonarny zestaw komputerowy – 25 sztuk** | |
|---|---|
| **Nazwa podzespołu** | **Minimalne wymagania parametry** |
| **Typ** | Komputer stacjonarny. Typu All in One, komputer wbudowany w monitor. W ofercie wymagane jest podanie modelu producenta komputera. |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| **Procesor** | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 8000 punktów |
| **Pamięć operacyjna RAM** | 8GB (1x8GB) DDR4 2400MHz non-ECC możliwość rozbudowy do min. 32GB |
| **Parametry pamięci masowej** | Min. 2.5" 500GB HDD |
| **Wydajność grafiki** | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1200 punktów w G3D Rating, wynik dostępny na stronie : http://www.videocardbenchmark.net/gpu_list.php |
| **Matryca** | Niedotykowa, antyodblaskowa matryca o przekątnej min. 21,5" (plamka max. 0,25mm) umożliwiająca wyświetlenie obrazu w 24-bitowej palecie kolorów (16,7 mln kolorów) o rozdzielczości FHD (1920x1080) przy częstotliwości odświeżania 60Hz, z czasem reakcji matrycy nie większym niż 25 ms. Jasność matrycy co najmniej 250 cd/m², kontrast co najmniej 600:1. Kąty widzenia pion/poziom min. 89/89 stopni. |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, 24-bitowa konwersja sygnału cyfrowego na analogowy i analogowego na cyfrowy; wbudowane dwa głośniki min. 2W na kanał;<br>Wbudowana w obudowę matrycy cyfrowa kamera z mikrofonem cyfrowym |

| | |
|---|---|
| | obsługujący poprawę mowy i redukcję szumów. Kamera wsparta o diodę LED informującą użytkownika o włączonej kamerze. Wbudowana w obudowę matrycy mechaniczna maskownica kamery. |
| **Obudowa** | Typu All-in-One zintegrowana z monitorem min. 21,5". Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) lub kłódki (oczko w obudowie do założenia kłódki),<br>Demontaż podstawy musi odbywać się bez użycia narzędzi, mocowanie jej opatrzone w przycisk zwalniający.<br>Podstawa musi oferować użytkownikowi możliwość regulacji w zakresie:<br>- przód/ tył – regulacja min. 35 stopni ( -5 / +30 )<br>- wysokości – min 100mm<br>- lewo/prawo – w zakresie min. 90 stopni ( 45 lewo / 45 prawo )<br>Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi, nie dopuszcza się stosowania śrub motylkowych, radełkowych czy zwykłych wkrętów. Suma wymiarów samej obudowy (bez podstawy) nie może przekraczać 99cm, Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100x100.<br>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, wpisanym na stałe w BIOS.<br>Zasilacz wewnętrzny o mocy max. 155W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%.<br>Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx. Do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80PLUS. W przypadku, kiedy u producenta występuje kilka zasilaczy, które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.<br>Wydruki 80PLUS muszą być potwierdzone przez producenta oświadczeniem producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają normę 80PLUS na zaoferowanym poziomie.<br>Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i dysku twardego bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych).<br>Obudowa musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.<br>Wbudowany wizualny system diagnostyczny w przycisku POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED przycisku POWER [tzn. barw i miganie] W szczególności musi sygnalizować:<br>▪ uszkodzenie lub brak pamięci RAM<br>▪ uszkodzenie płyty głównej [w tym również portów I/O, chipset]<br>▪ uszkodzenie kontrolera Video<br>▪ awarię BIOS'u<br>▪ awarię procesora<br>Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej niewymienionych w specyfikacji, a które nie są dedykowane dla systemu diagnostycznego.<br>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| **Zgodność z systemami operacyjnymi i standardami** | Potwierdzenie kompatybilności komputera z zaoferowaną platformę systemową (wydruk ze strony) |

| | |
|---|---|
| **Bezpieczeństwo** | Wlutowany w płytę główną (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiekolwiek złącza wyprowadzone na płycie) dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej.<br>Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot'owania umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności:<br>▪ testy uruchamiane automatycznie lub w trybie interaktywnym<br>▪ możliwość powtórzenia testów<br>▪ podsumowanie testów z możliwością zapisywania wyników<br>▪ uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu,<br>▪ uruchamianie testów zdefiniowanych przez użytkownika<br>▪ wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów<br>▪ wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.<br>Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera, podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, typ pamięci wraz z taktowaniem oraz SN i PN, wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz.<br>Zasilacz wyposażony w swój własny system diagnostyczny niezależny od pozostałych komponentów oferowanego komputera umożliwiający sprawdzenie poprawnego funkcjonowania zasilacza bez narażania pozostałych składowych na ewentualne uszkodzenia (przepięcia itp.)<br>Czujnik otwarcia obudowy musi zbierać logi i zapisywać je w BIOS |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera,<br>Pełna obsługa BIOS za pomocą klawiatury i myszy, bądź też samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:<br>▪ wersji BIOS,<br>▪ nr seryjnym komputera,<br>▪ dacie wyprodukowania komputera,<br>▪ ilości zainstalowanej pamięci RAM,<br>▪ prędkości zainstalowanych pamięci RAM,<br>▪ technologii wykonania pamięci, |

| | |
|---|---|
| | ▪ sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki: DIIMM 1, DIMM 2,<br>▪ typie zainstalowanego procesora,<br>▪ ilości rdzeni zainstalowanego procesora,<br>▪ typowej prędkości zainstalowanego procesora<br>▪ minimalnej osiąganej prędkości zainstalowanego procesora,<br>▪ maksymalnej osiąganej prędkości zainstalowanego procesora,<br>▪ pamięci cache L2 zainstalowanego procesora,<br>▪ pamięci cache L3 zainstalowanego procesora,<br>▪ zainstalowanych dyskach twardych, w tym informacja o pojemności, PN dysku<br>▪ MAC adresie zintegrowanej karty sieciowej,<br>▪ zintegrowanym układzie graficznym,<br>▪ kontrolerze audio<br><br>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.<br>Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego.<br>Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.<br>Możliwość włączenia/wyłączenia kontrolera audio, klawiszy OSD, dotyku ekranu (funkcja na stałe zaimplementowana w BIOS, ale dostępna i aktywna tylko dla matrycy dotykowej), wbudowanej kamery.<br>Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.<br>Możliwość włączenia/wyłączenia funkcji umożliwiającej dokonywanie downgrade’u BIOS,<br>Możliwość włączenia/wyłączenia funkcji tworzenia recovery BIOS na dysku twardym,<br>Możliwość wyłączania portów USB w tym:<br>▪ wszystkich portów USB 2.0 i 3.0,<br>▪ tylko portów USB znajdujących się na przednim panelu obudowy,<br>▪ tylko portów USB znajdujących się na tylnym panelu obudowy.<br>▪ tylko tylnych portów USB 2.0, porty USB 3.0 na panelu tylnym aktywne,<br>▪ pojedynczo portów USB<br><br>Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego bootowania które umożliwia m.in.:<br>▪ uruchamianie systemu zainstalowanego na HDD<br>▪ uruchamianie systemu z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, CDRW-USB<br>▪ uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej<br>▪ uruchamianie systemu z karty SD (funkcja aktywna automatycznie po zainstalowaniu karty SD w czytniku [w przypadku zainstalowania czytnika kart w komputerze] |

| | |
|---|---|
| | ▪ uruchomienie graficznego systemu diagnostycznego<br>▪ wejścia do BIOS<br>▪ upgrade BIOS bez konieczności uruchamiania systemu operacyjnego<br>▪ zmiany sposobu bootowania z Legacy na UEFI lub z UEFI na Legacy bez konieczności wchodzenia do BIOS. |
| **Certyfikaty i standardy** | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)<br>Deklaracja zgodności CE (załączyć do oferty)<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram<br>Certyfikat TCO, wymagany wpis na stronie: http://tco.brightly.se/pls/nvp/!tco_search – załączyć do oferty wydruk z strony<br>Komputer musi spełniać wymogi normy Energy Star 6.0. Dołączony do oferty certyfikat potwierdzony przez producenta lub wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov (wydruk ze strony internetowej) |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB (załączyć oświadczenie producenta) |
| **Warunki gwarancji** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.<br>W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.<br>Do oferty wymagane jest dołączenie oświadczenie producenta komputera, że w przypadku niewywiązania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej przejmie na siebie wszelkie zobowiązania związane z serwisem. |
| **Wsparcie techniczne producenta** | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.<br>Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |
| **System Operacyjny** | Zainstalowany system operacyjny Windows 10 Professional + nośnik, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub rozwiązanie równoważne. |
| **Oprogramowanie biurowe** | Licencja pakietu biurowego zgodnego ze specyfikacją, poz. 8 – Pakiet oprogramowania biurowego; pakiet preinstalowany przez producenta komputera |
| **Złącza i porty** | Wbudowane porty:<br>• min. 1 x HDMI 1.4<br>• min. 1 x DP 1.2<br>• min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0; min. 2 porty USB 3.0 usytuowane na boku obudowy i 4 portów na |

| | |
|---|---|
| | tylnym panelu w tym min 2 porty USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.)<br>• 2 porty audio w kombinacji 1x in i 1x out<br>• Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika),<br>• Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w :<br>min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM,<br>min. 2 złącza SATA 3.0;<br>min. 1 złącze M.2 2280 PCI-Express x4<br>min. 1 złącze M.2 dedykowane dla karty WiFi<br>• Klawiatura USB w układzie polski programisty<br>• Czytnik kart multimedialnych czytający min. karty SD (wszystkie ich odmiany)<br>• Mysz optyczna USB z sześcioma klawiszami oraz rolką (scroll) min. 1000dpi<br>• Nagrywarka DVD +/-RW o prędkości min. 8x |
| **Dodatkowe oprogramowanie** | Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie:<br>▪ umożliwiające upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS-u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,<br>▪ posiadające możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS-u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :<br>a. o poprawkach i usprawnieniach dotyczących aktualizacji<br>b. dacie wydania ostatniej aktualizacji<br>c. priorytecie aktualizacji<br>d. zgodność z systemami operacyjnymi<br>e. jakiego komponentu sprzętu dotyczy aktualizacja<br>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.<br>• sporządzające wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne<br>• posiadające możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika lub aplikacji, która tego wymaga.<br>• rozpoznające model oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)<br>• umożliwiające sprawdzenie historii upgrade'u z informacją, jakie sterowniki były instalowane wraz z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania )<br>• sporządzające dokładny wykaz wymaganych sterowników, aplikacji, BIOS-u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml<br>• sporządzające raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |

| 5. Laptop – 4 sztuk | |
|---|---|
| **Nazwa podzespołu** | **Minimalne wymagania parametry** |
| **Zastosowanie** | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| **Przekątna ekranu** | FHD (1920 x 1080) z podświetleniem LED i powłoką przeciwodblaskową, jasność 220 nits, kontrast 400:1 , maksymalny rozmiar plamki 0,180mm |
| **Procesor** | Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 4680 punktów Passmark CPU Mark.<br>Wynik dostępny na stronie: http://www.passmark.com/products/pt.htm |
| **Płyta główna** | Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta i oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera. |
| **Pamięć RAM** | 8GB (1x8GB) DDR4 2133MHz możliwość rozbudowy do min 32GB, wymagane min. 2 sloty na pamięci w tym min. jeden wolny |
| **Pamięć masowa** | Min. 500 GB HDD |
| **Karta graficzna** | Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej,<br>Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 930 punktów w G3D Rating, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php |
| **Klawiatura** | Klawiatura wyspowa z wydzielą z prawej strony klawiaturą numeryczną, z wbudowanym w klawiaturze podświetleniem z możliwością manualnej regulacji zarówno w BIOS jak i z pod systemu operacyjnego, (układ US -QWERTY), min 100 klawiszy. |
| **Multimedia** | dwukanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy 2x 2W.<br>Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.<br>Kamera internetowa z diodą informującą o aktywności, o rozdzielczości min. 1280x720 trwale zainstalowana w obudowie matrycy. |
| **Bateria i zasilanie** | Co najmniej czterokomorowa [min. 56Wh]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.<br>Zasilacz o mocy min. 65W. |
| **Waga i wymiary** | Waga max 2,3kg z baterią<br>Szerokość: max 380 mm<br>Wysokość: max 25 mm<br>Głębokość: max 260 mm |
| **Obudowa** | Szkielet obudowy i zawiasy notebooka wykonany z wzmacnianego metalu. Kąt otwarcia notebooka min. 140 stopni. |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **BIOS** | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i myszy oraz urządzenia wskazującego zintegrowanego (wmontowanego na stałe) oraz samej myszy.<br>Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:<br>▪ wersji BIOS,<br>▪ nr seryjnego komputera, |

| | |
|---|---|
| | ▪ numeru wpisanego i nadanego przez administratora (o ile został wpisany, jeśli brak – wymaga się wolnego pola)<br>▪ dacie produkcji komputera<br>▪ całkowitej wielkości zainstalowanej pamięci RAM,<br>▪ prędkości zainstalowanej pamięci RAM<br>▪ technologii wykonania pamięci RAM<br>▪ sposobu obsadzenia slotów DIMM z rozbiciem na bank A i B (w przypadku obsadzenia tylko jednej kości pamięci drugi bank wolne pole)<br>▪ typie zainstalowanego procesora<br>▪ liczbie rdzeni procesora<br>▪ minimalnej prędkości zegara procesora<br>▪ maksymalnej prędkości zegara procesora<br>▪ wielkości pamięci podręcznej procesora L2 cache<br>▪ wielkości pamięci podręcznej procesora L3 cache<br>▪ zainstalowanym i podpiętym HDD (mini SSD)<br>▪ kontrolerze video<br>▪ wersji BIOS kontrolera video<br>▪ pamięci kontrolera video przydzielonej na poziomie BIOS-u<br>▪ typie zainstalowanego w komputerze panelu LCD (wielkość matrycy w calach)<br>▪ natywnej rozdzielczości zainstalowanego w komputerze panelu LCD<br>▪ kontrolerze audio<br>▪ zainstalowanej karcie Wifi (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole)<br>▪ zainstalowanym Bluetooth (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole)<br>▪ MAC adresie wbudowanej w płytę główną karty sieciowej<br>▪ poziomie naładowania baterii zainstalowanej i obecnie użytkowanej w komputerze,<br>▪ czy komputer pracuje na zasilaniu z baterii lub na podłączonym zasilaczu<br>▪ funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń zewnętrznych urządzeń. |
| **Certyfikaty** | Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty)<br>Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty)<br>Deklaracja zgodności CE (załączyć do oferty)<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki<br>Potwierdzenie kompatybilności komputera na stronie Windows Logo'd Products List na daną platformę systemową (wydruk ze strony)<br>EnergyStar 6.0 – dołączony do oferty certyfikat potwierdzony przez producenta lub wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov (wydruk ze strony internetowej) podparty oświadczeniem producenta.<br>Certyfikat TCO, wymagany wpis na stronie : http://tco.brightly.se/pls/nvp/!tco_search – załączyć do oferty wydruk z strony |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 17dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta). |

| | |
|---|---|
| **Diagnostyka** | Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności:<br>▪ testy uruchamiane automatycznie lub w trybie interaktywnym<br>▪ możliwość powtórzenia testów<br>▪ podsumowanie testów z możliwością zapisywania wyników<br>▪ uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu,<br>▪ uruchamianie testów zdefiniowanych przez użytkownika<br>▪ wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów<br>▪ wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.<br>Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera.<br>Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o natywnej rozdzielczości matrycy, numerze seryjnym, typie i pojemności dysku twardego, o żywotności baterii – informacja podana w %, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, typ pamięci wraz z taktowanie oraz SN i PN, wykaz temperatur dla baterii, CPU, pamięci, temperatury panującej wewnątrz.<br>W przypadku braku możliwości uruchomienia graficznego systemu diagnostycznego komputer musi zawierać w sobie dodatkowo niezależny system diagnostyczny wizualny oparty o sygnalizację świetlną informujący użytkownika o :<br>▪ awarii procesora<br>▪ awarii płyty głównej<br>▪ awarii chipsetu płyty głównej<br>▪ braku pamięci RAM, niewykryciu pamięci RAM<br>▪ awarii pamięci RAM<br>▪ nieprawidłowym lub nieprawidłowej zainstalowanej pamięci RAM<br>▪ awarii matrycy LCD<br>▪ awarii baterii CMOS<br>▪ awarii układu graficznego<br>▪ uszkodzeniu obrazu BIOS<br>▪ nieodnalezieniu obrazu BIOS |
| **Bezpieczeństwo** | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.<br>Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.<br>Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy.<br>Czytnik linii papilarnych<br>Złącze typu Security Lock |
| **System operacyjny** | Zainstalowany system operacyjny Windows 10 Professional + nośnik, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub rozwiązanie równoważne. |

| | |
|---|---|
| **Oprogramowanie biurowe** | Licencja pakietu biurowego zgodnego ze specyfikacją, poz. 8 – Pakiet oprogramowania biurowego; pakiet preinstalowany przez producenta komputera |
| **Dodatkowe oprogramowanie dodatkowe** | Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasową na użytkowanie:<br>▪ umożliwiające upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS-u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,<br>▪ posiadające możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS-u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:<br>a. o poprawkach i usprawnieniach dotyczących aktualizacji<br>b. dacie wydania ostatniej aktualizacji<br>c. priorytecie aktualizacji<br>d. zgodność z systemami operacyjnymi<br>e. jakiego komponentu sprzętu dotyczy aktualizacja<br>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.<br>▪ sporządzające wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne<br>▪ posiadające możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika lub aplikacji, która tego wymaga.<br>▪ rozpoznające model oferowanego komputera, numer seryjny komputera, informację, kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)<br>▪ umożliwiające sprawdzenie historii upgrade'u z informacją, jakie sterowniki były instalowane wraz z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)<br>▪ sporządzające dokładny wykaz wymaganych sterowników, aplikacji, BIOS-u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml<br>▪ sporządzające raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.<br>Dołączone do oferowanego komputera oprogramowanie antywirusowe |
| **Porty i złącza** | Wbudowane porty i złącza :<br>▪ 1x VGA<br>▪ 1x HDMI 1.4<br>▪ 1x RJ-45 (10/100/1000)<br>▪ 2x USB 3.1, jeden port dosilony<br>▪ 1x USB 2.0<br>▪ czytnik kart multimedialny wspierający karty SD 4.0<br>▪ czytnik linii papilarnych<br>▪ współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo<br>▪ port zasilania<br>▪ touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów<br>▪ zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN AC z modułem Bluetooth min. 4.1 |

| | |
|---|---|
| **Warunki gwarancyjne** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.<br>W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.<br>Do oferty wymagane jest dołączenie oświadczenie producenta komputera, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej przejmie na siebie wszelkie zobowiązania związane z serwisem. |

| **6. Macierz dyskowa – 1 sztuka** | |
|---|---|
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19". Wysokość maksymalnie 2U wraz z kompletem szyn do montażu w szafie Rack z możliwością instalacji minimum 12 dysków 3.5" Hot Plug. |
| **Kontrolery** | Dwa kontrolery posiadające łącznie minimum osiem portów FC minimum 16 Gb/s wraz z 4 wkładkami SFP do podłączenia serwerów, pracujące w trybie active-active.<br>Wymagane poziomy zabezpieczenia RAID: 0,1,5,6,10.<br>Minimum 4GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inną pamięć nieulotną lub podtrzymywana bateryjnie przez min. 72h w razie awarii. |
| **Dyski twarde** | Zainstalowane dyski:<br>4 dyski o pojemności minimum 4TB NearLine SAS 7.2k Hot-Plug 3.5" każdy.<br>Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 190 dysków, wydajnych dysków SAS, SSD, ekonomicznych dysków typu SATA (lub NearLine SAS), samoszyfrujących dysków SED dostępnych w ofercie producenta macierzy, możliwość mieszania typów dysków w obrębie macierzy oraz półki. |
| **Oprogramowanie** | Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków.<br>Możliwość rozbudowy o licencję umożliwiającą utworzenie minimum 512 LUN'ów oraz 32 kopii migawkowych na LUN.<br>Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 32 hostów bez konieczności zakupu dodatkowych licencji.<br>Zarządzanie macierzą poprzez minimum oprogramowanie zarządzające lub przeglądarkę internetową. Wymagana funkcja paska postępu – progress bar'u lub wyświetlenia wartości zaawansowania operacji w procentach przypadku formatowania wirtualnych dysków w oparciu o fizyczne dyski zainstalowane w macierzy.<br>Dodatkowe oprogramowanie umożliwiające wspólne zarządzanie oferowanymi serwerami oraz oferowaną macierzą poprzez sieć spełniające minimalne wymagania:<br>- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych<br>- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta<br>- Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH<br>- Możliwość oskryptowywania procesu wykrywania urządzeń<br>- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram<br>- Szczegółowy opis wykrytych systemów oraz ich komponentów<br>- Możliwość eksportu raportu do CSV, HTML, XLS<br>- Grupowanie urządzeń w oparciu o kryteria użytkownika<br>- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach<br>- Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń |

| | |
|---|---|
| | - Szybki podgląd stanu środowiska<br>- Podsumowanie stanu dla każdego urządzenia<br>- Szczegółowy status urządzenia/elementu/komponentu<br>- Generowanie alertów przy zmianie stanu urządzenia<br>- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń<br>- Integracja z service desk producenta dostarczonej platformy sprzętowej<br>- Możliwość przejęcia zdalnego pulpitu<br>- Możliwość podmontowania wirtualnego napędu<br>- Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu<br>- Kreator umożliwiający dostosowanie akcji dla wybranych alertów<br>- Możliwość importu plików MIB<br>- Przesyłanie alertów „as-is" do innych konsol firm trzecich<br>- Możliwość definiowania ról administratorów<br>- Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów<br>- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)<br>- Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta<br>- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów<br>- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych. |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.<br>Możliwość przydzielenia większej przestrzeni dyskowej dla serwerów niż fizycznie dostępna (Thin Provisioning)<br>Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników. |
| **Warunki gwarancji** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.<br>W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.<br>Do oferty wymagane jest dołączenie oświadczenie producenta komputera, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej przejmie na siebie wszelkie zobowiązania związane z serwisem.<br>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. |
| **Dokumentacja** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Certyfikaty** | Macierz wyprodukowana zgodnie z normą ISO 9001:2008 oraz 14001<br>Zgodność z systemami operacyjnymi: Microsoft® Windows®, VMware®, Microsoft Hyper-V®, Citrix® XenServer®, Red Hat® oraz SUSE |

| **7. Przełącznik Fibre Channel – 1 sztuka** | |
|---|---|
| **Lp.** | **Minimalne wymagania w zakresie parametrów technicznych** |

| | |
|---|---|
| 1. | Przełącznik FC musi być wykonany w technologii FC 8 Gb/s i posiadać możliwość pracy portów FC z prędkościami 8, 4, 2 Gb/s z funkcją autonegocjacji prędkości. |
| 2. | Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 8 portów FC przełącznika. |
| 3. | Przełącznik musi być dostarczony wraz z minimum 8 modułami SFP FC 8 Gb/s. |
| 4. | Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| 5. | Przełącznik FC musi posiadać nadmiarowe wentylatory N+1. |
| 6. | Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. |
| 7. | Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach. |
| 8. | Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. |
| 9. | Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. |
| 10. | Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:<br>▪ Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric<br>▪ Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP<br>▪ Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP<br>▪ Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów<br>▪ Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,<br>▪ Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric.<br>▪ Konta użytkowników definiowane w środowisku RADIUS lub LDAP<br>▪ Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS<br>▪ Obsługa SNMP v3 |
| 11. | Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. |
| 12. | Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. |
| 13. | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC |
| 14. | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1) |
| 15. | Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP |
| 16. | Maksymalny dopuszczalny pobór mocy przełącznika FC to 57W |
| 17. | Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. |
| 18. | Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns. |
| 19. | Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN |
| 20. | Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID. |
| 21. | Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). |

| | |
|---|---|
| 22. | Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
| 23. | Być objęty gwarancją na sprzęt przynajmniej na pięć lat. Gwarancja powinna być świadczona w trybie co najmniej 365x7x24, z czterogodzinnym czasem reakcji . |
| 24. | Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. |
| 25. | Szyny do montażu w szafie rack. |

| **8. Serwerowy system operacyjny – 1 sztuka** | |
|---|---|
| **Lp.** | **Minimalne wymagania w zakresie parametrów technicznych** |
| 1. | Licencja na serwerowy system operacyjny musi być przypisana do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym. |
| 2. | Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. |
| 3. | Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. |
| 4. | Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. |
| 5. | Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |
| 6. | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |
| 7. | Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |
| 8. | Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
| 9. | Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. |
| 10. | Wbudowane wsparcie instalacji i pracy na wolumenach, które:<br>a. pozwalają na zmianę rozmiaru w czasie pracy systemu,<br>b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,<br>c. umożliwiają kompresję w locie; dla wybranych plików i/lub folderów,<br>d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
| 11. | Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |
| 12. | Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |
| 13. | Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET |
| 14. | Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów |
| 15. | Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych |
| 16. | Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych |
| 17. | Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe |
| 18. | Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji |

| | |
|---|---|
| 19. | Mechanizmy logowania w oparciu o:<br>a. Login i hasło,<br>b. Karty z certyfikatami (smartcard),<br>c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), |
| 20. | Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. |
| 21. | Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
| 22. | Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
| 23. | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
| 24. | Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). |
| 25. | Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |
| 26. | Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:<br>a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,<br>b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:<br>i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,<br>ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,<br>iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.<br>iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. lub wyższy<br>c. Zdalna dystrybucja oprogramowania na stacje robocze.<br>d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej<br>e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<br>i. Dystrybucję certyfikatów poprzez http<br>ii. Konsolidację CA dla wielu lasów domeny,<br>iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,<br>iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.<br>f. Szyfrowanie plików i folderów.<br>g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).<br>h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.<br>i. Serwis udostępniania stron WWW.<br>j. Wsparcie dla protokołu IP w wersji 6 (IPv6),<br>k. Wsparcie dla algorytmów Suite B (RFC 4869),<br>l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,<br>m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej |

| | |
|---|---|
| | funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:<br>i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,<br>ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.<br>iii. Obsługi 4-KB sektorów dysków<br>iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra<br>v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.<br>vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) |
| 27. | Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. |
| 28. | Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). |
| 29. | Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. |
| 30. | Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
| 31. | Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| 32. | Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

| **9. Oprogramowanie antywirusowe – 29 szt.** | |
|---|---|
| **Nazwa składnika/parametru technicznego** | **Minimalne wymagania w zakresie parametrów technicznych** |
| Wsparcie dla systemów operacyjnych | • Microsoft Windows 10 Pro x86 / x64<br>• Microsoft Windows 10 Enterprise x86 / x64<br>• Microsoft Windows 8.1 Pro x86 / x64<br>• Microsoft Windows 8.1 Enterprise x86 / x64<br>• Microsoft Windows 8 Pro x86 / x64<br>• Microsoft Windows 8 Enterprise x86 / x64<br>• Microsoft Windows 7 Professional x86 / x64 SP1 lub nowszy<br>• Microsoft Windows 7 Enterprise / Ultimate x86 / x64 SP1 lub nowszy<br>• Microsoft Windows 7 Professional x86 / x64<br>• Microsoft Windows 7 Enterprise / Ultimate x86 / x64 |
| Informacje ogólne | • Polskojęzyczny interfejs konsoli zarządzającej i programu na stacjach roboczych.<br>• Program powinien posiadać certyfikaty niezależnych laboratoriów.<br>• Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.<br>• Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony. |
| Ochrona w czasie rzeczywistym | • Program ma możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury.<br>• Program ma możliwość wyświetlenia podsumowania o aktywności, reputacji i lukach w aplikacjach aktualnie uruchomionych w systemie.<br>• Program ma możliwość monitorowania prób uruchamiania aplikacji przez |

| | |
|---|---|
| | użytkowników zgodnie z określonymi regułami.<br>• Program ma możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.<br>• Program posiada dedykowany moduł blokujący określone kategorie urządzeń (np. pamięci masowe, urządzenia Bluetooth itp.).<br>▪ Możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik, określenia przedziału czasu, w którym użytkownik będzie miał możliwość tylko zapisu bądź tylko odczytu, ewentualnie zapisu i odczytu.<br>▪ Możliwość blokowania urządzeń według ich rodzaju: dyski, USB, drukarki itp. w zależności od czasu, konta użytkownika systemu Windows oraz rodzaju operacji: odczyt/zapis.<br>▪ Możliwość utworzenia listy zaufanych urządzeń na podstawie modelu, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.<br>• Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego urządzenia; nośnik wymienny, napęd CD-ROM itd.<br>• Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego zasobu sieciowego.<br>• Użytkownik, ma możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanej aplikacji.<br>• Kontrola sieci – kontrola dostępu do zasobów sieciowych w zależności od ich zawartości i lokalizacji:<br>▪ Możliwość definiowania reguł filtrujących zawartość na wybranej stronie lub wszystkich stronach w zależności od kategorii zawartości: pornogafia, narkotyki, broń, gry, sieci społecznościowe, banery, itd.<br>▪ Możliwość definiowania reguł blokujących bądź zezwalających na wyświetlanie określonej treści na wybranej stronie lub wszystkich stronach w zależności od kategorii danych: pliki wideo, audio, archiwa itd.<br>• Monitor wykrywania luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.<br>• Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX).<br>• Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.<br>• Wbudowany moduł skanujący protokoły POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.<br>• Skaner poczty powinien mieć możliwość zmiany nazwy lub usuwania określonych typów załączników.<br>• Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.<br>• Wbudowany moduł skanujący ruch komunikatorów ICQ, MSN, AIM, Mail.Ru Agent oraz IRC.<br>• Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.<br>• Możliwość określenia poziomu czułości modułu heurystycznego.<br>• Wbudowany moduł skanujący skrypty napisane w językach VB Script i Java Script wykonywane przez system operacyjny Windows oraz program Internet Explorer.<br>• Wbudowany moduł kontrolujący dostęp do rejestru systemowego. |

| | |
|---|---|
| | • Wbudowany moduł kontrolujący dostęp do ustawień Internet Explorera.<br>• Wbudowany moduł chroniący przed phishingiem.<br>• Moduł zapory ogniowej z możliwością:<br>▪ Tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji.<br>▪ Tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP.<br>▪ Zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory<br>• Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów.<br>• Kontrola systemu poprzez ochronę proaktywną przed nowymi zagrożeniami, które nie znajdują się w antywirusowych bazach danych:<br>▪ Kontrola aktywności aplikacji, dostarczanie szczegółowych informacji dla innych modułów aplikacji w celu zapewnienia jeszcze bardziej efektywnej ochrony.<br>▪ Możliwość wycofywania zmian wprowadzanych w systemie przez szkodliwe oprogramowanie nawet w poprzednich sesjach logowania.<br>• Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.<br>• Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.<br>• Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.<br>• Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.<br>• Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.<br>• Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.<br>• Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie bądą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.<br>• Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.<br>• Program posiada funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.<br>• Program posiada możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.<br>• Program posiada możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.<br>• Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu przy użyciu zdefiniowanej nazwy użytkownika i hasła.<br>• Program ma możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej).<br>• Program powinien zapewnić autoryzację urządzeń typu klawiatura podłączanych do portu USB.<br>• Jeżeli podłączane urządzenie nie posiada fizycznych klawiszy np. czytnik |

| | |
|---|---|
| | kodów kreskowych, program powinien zapewnić możliwość autoryzacji urządzenia przy użyciu klawiatury ekranowej. |
| Skanowanie na żądanie | • Skanowanie w czasie rzeczywistym:<br>▪ Uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików.<br>▪ Pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.<br>▪ Plików pobieranych z Internetu po protokole HTTP.<br>▪ Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego.<br>▪ Treści i plików przesyłanych z wykorzystaniem komunikatorów ICQ, MSN, AIM, Mail.Ru Agent oraz IRC.<br>• W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:<br>▪ Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt<br>▪ Rejestrować w pliku raportu informację o wykryciu wirusa<br>▪ Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND<br>▪ Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku<br>▪ Poddać kwarantannie podejrzany obiekt<br>• Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.<br>• Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania.<br>• System antywirusowy posiada możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia. |
| Aktualizacja baz danych sygnatur zagrożeń | • Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.<br>• Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.<br>• Program powinien posiadać możliwość określenia źródła uaktualnień.<br>• Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.<br>• Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.<br>• Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.<br>• Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia<br>• z Internetem.<br>• Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji). |
| Raportowanie | • Program powinien posiadać możliwość raportowania zdarzeń informacyjnych.<br>• Program powinien posiadać możliwość określenia okresu przechowywania raportów.<br>• Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie. |

| | |
|---|---|
| Dodatkowa konfiguracja | • Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na bateriach.<br>• Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.<br>• Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.<br>• Program musi mieć możliwość włączenia opcji współdzielenia zasobów z innymi apikacjami. |
| System scentralizowanego zarządzania – wsparcie dla systemów operacyjnych | System scentralizowanego zarządzania powinien obsługiwać następujące systemy operacyjne:<br>• Microsoft Windows 10 Pro 32-bitowy / 64-bitowy<br>• Microsoft Windows 10 RS2 32-bitowy / 64-bitowy<br>• Microsoft Windows 10 Enterprise 32-bitowy / 64-bitowy<br>• Microsoft Windows 10 Education 32-bitowy / 64-bitowy<br>• Microsoft Windows 10 Pro RS1 32-bitowy / 64-bitowy<br>• Microsoft Windows 10 Enterprise RS1 32-bitowy / 64-bitowy<br>• Microsoft Windows 10 Education RS1 32-bitowy / 64-bitowy<br>• Microsoft Windows 8.1 Pro 32-bitowy / 64-bitowy<br>• Microsoft Windows 8.1 Enterprise 32-bitowy / 64-bitowy<br>• Microsoft Windows 8 Pro 32-bitowy / 64-bitowy<br>• Microsoft Windows 8 Enterprise 32-bitowy / 64-bitowy<br>• Microsoft Windows 7 Professional SP1 32-bitowy / 64-bitowy<br>• Microsoft Windows 7 Enterprise SP1 32-bitowy / 64-bitowy<br>• Microsoft Windows 7 Ultimate SP1 32-bitowy / 64-bitowy<br>• Microsoft Small Business Server 2008 Standard 64-bit<br>• Microsoft Small Business Server 2008 Premium 64-bitowy<br>• Microsoft Small Business Server 2011 Essentials 64-bitowy<br>• Microsoft Small Business Server 2011 Premium Add-on 64-bitowy<br>• Microsoft Small Business Server 2011 Standard 64-bitowy<br>• Microsoft Windows Server 2008 Datacenter SP1 32-bitowy / 64-bitowy<br>• Microsoft Windows Server 2008 Enterprise SP1 32-bitowy / 64-bitowy<br>• Microsoft Windows Server 2008 Foundation SP2 32-bitowy / 64-bitowy<br>• Microsoft Windows Server 2008 SP1 32-bitowy / 64-bitowy<br>• Microsoft Windows Server 2008 Standard SP1 32-bitowy / 64-bitowy<br>• Microsoft Windows Server 2008<br>• Microsoft Windows Server 2008 R2 Server Core 64-bitowy<br>• Microsoft Windows Server 2008 R2 Datacenter 64-bitowy<br>• Microsoft Windows Server 2008 R2 Datacenter SP1 64-bitowy<br>• Microsoft Windows Server 2008 R2 Enterprise 64-bitowy<br>• Microsoft Windows Server 2008 R2 Enterprise SP1 64-bitowy<br>• Microsoft Windows Server 2008 R2 Foundation 64-bitowy<br>• Microsoft Windows Server 2008 R2 Foundation SP1 64-bitowy<br>• Microsoft Windows Server 2008 R2 SP1 Core Mode 64-bitowy<br>• Microsoft Windows Server 2008 R2 Standard 64-bitowy<br>• Microsoft Windows Server 2008 R2 Standard SP1 64-bit<br>• Microsoft Windows Server 2012 Server Core 64-bitowy<br>• Microsoft Windows Server 2012 Datacenter 64-bitowy<br>• Microsoft Windows Server 2012 Essentials 64-bitowy<br>• Microsoft Windows Server 2012 Foundation 64-bitowy |

| | |
|---|---|
| | • Microsoft Windows Server 2012 Standard 64-bitowy<br>• Microsoft Windows Server 2012 R2 Server Core 64-bitowy<br>• Microsoft Windows Server 2012 R2 Datacenter 64-bitowy<br>• Microsoft Windows Server 2012 R2 Essentials 64-bitowy<br>• Microsoft Windows Server 2012 R2 Foundation 64-bitowy<br>• Microsoft Windows Server 2012 R2 Standard 64-bitowy<br>• Windows Storage Server 2008 R2 64-bitowy<br>• Windows Storage Server 2012 64-bitowy<br>• Windows Storage Server 2012 R2 64-bitowy<br>• Microsoft Windows Server 2016 64-bitowy |
| System scentralizowanego zarządzania – wsparcie dla baz danych | System scentralizowanego zarządzania powinien przechowywać ustawienia w relacyjnej bazie danych:<br>• Microsoft SQL Server 2008 Express 32-bitowy<br>• Microsoft SQL 2008 R2 Express 64-bitowy<br>• Microsoft SQL 2012 Express 64-bitowy<br>• Microsoft SQL 2014 Express 64-bitowy<br>• Microsoft SQL Server 2008 (wszystkie wersje) 32-bitowy / 64-bitowy<br>• Microsoft SQL Server 2008 R2 (wszystkie wersje) 64-bitowy<br>• Microsoft SQL Server 2008 R2 Service Pack 2 64-bitowy<br>• Microsoft SQL Server 2012 (wszystkie wersje) 64-bitowy<br>• Microsoft SQL Server 2014 (wszystkie wersje) 64-bitowy<br>• Microsoft SQL Server 2016 (wszystkie wersje) 64-bitowy<br>• Microsoft Azure SQL Database<br>• MySQL 5.5 32-bitowy / 64-bitowy<br>• MySQL Enterprise 5.5 32-bitowy / 64-bitowy<br>• MySQL 5.6 32-bitowy / 64-bitowy<br>• MySQL Enterprise 5.6 32-bitowy / 64-bitowy<br>• MySQL 5.7 32-bit / 64-bit; MySQL Enterprise 5.7 32-bitowy / 64-bitowy |
| System scentralizowanego zarządzania - funkcje | • System zdalnego zarządzania powinien posiadać polskojęzyczny interfejs konsoli programu.<br>• System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory).<br>• System zdalnego zarządzania powinien umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły.<br>• System zdalnego zarządzania powinien posiadać jeden pakiet instalacyjny dla stacji roboczej jak również systemów serwerowych.<br>• System zdalnego zarządzania powinien umożliwiać ograniczenie pasma sieciowego wykorzystywanego do komunikacji stacji z serwerem administracyjnych. Reguły powinny umożliwić ograniczenia w oparciu o zakresy adresów IP oraz przedziały czasowe.<br>• System zdalnego zarządzania umożliwia tworzenie hierarchicznej struktury serwerów administracyjnych jak również tworzenie wirtualnych serwerów administracyjnych.<br>• System zdalnego zarządzania umożliwia zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.<br>• Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych jest szyfrowana przy użyciu protokołu SSL.<br>• Konsola administracyjna posiada możliwość zdalnego inicjowania |

| | |
|---|---|
| | skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie.<br>• Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.<br>• Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa.<br>• Serwer zarządzający ma możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).<br>• System centralnego zarządzania wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych.<br>• System centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.<br>• System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie\<br>• i zainstalowanie nowego oprogramowania.<br>• Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.<br>• System centralnego zarządzania powinien zapewniać obsługę trybu dynamicznego dla Virtual Desktop Infrastructure (VDI).<br>• System centralnego zbierania informacji i tworzenia sumarycznych raportów.<br>• System zdalnego zarządzania powinien umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formatach HTML, XML i PDF).<br>• System zdalnego zarządzania powinien umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.<br>• System zdalnego zarządzania powinien umożliwiać tworzenie kategorii aplikacji i warunków ich uruchomienia.<br>• System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o aplikacjach i plikach wykonywalnych znajdujących się na stacjach roboczych.<br>• Program powinien mieć możliwość dezinstalacji aplikacji niekompatybilnych jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika.<br>• System zdalnego zarządzania powinien wyświetlać szczegółowe informacje na temat luk w oprogramowaniu wykrytych na zarządzanych komputerach<br>• System zdalnego zarządzania powinien mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.<br>• System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.).<br>• System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o kopiach zapasowych obiektów wyleczonych/usuniętych na stacjach roboczych wraz z możliwością ich przywrócenia do początkowej lokalizacji i/lub zapisania na stacji administratora.<br>• System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania. |

| | |
|---|---|
| | • System zdalnego zarządzania powinien umożliwiać automatyczne instalowanie licencji na stacjach roboczych.<br>• System zdalnego zarządzania powinien umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania.<br>• System zdalnego zarządzania powinien umożliwiać automatyczne uruchomienie wyłączonych komputerów przed wykonaniem odpowiednich zadań administracyjnych (z wykorzystaniem funkcji Wake-On-LAN) a po zakończeniu wykonywania zadań ich wyłączenie. Funkcjonalność ta nie może być ograniczona tylko do podsieci, w której znajduje się serwer administracyjny.<br>• System zdalnego zarządzania powinien umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści.<br>• System zdalnego zarządzania powinien umożliwiać zdalne włączanie, wyłączanie oraz restartowanie komputerów wraz z możliwością interakcji z użytkownikiem (np. natychmiastowe wykonanie działania lub jego odłożenie na zdefiniowany okres czasu).<br>• Program powinien umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji, ikony w pasku systemowym, wpisów w Menu Start oraz na liście zainstalowanych programów.<br>• Program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.<br>• System zdalnego zarządzania powinien umożliwiać administrację poprzez przeglądarkę internetową.<br>• System zdalnego zarządzania powinien dać możliwość wykorzystania bramy połączenia dla komputerów, które nie mają bezpośredniego połączenia z Serwerem administracyjnym.<br>• System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.<br>• System zdalnego zarządzania powinien tworzyć listę kont użytkowników sieci. Do tworzenia powinny być wykorzystywane różne źródła w tym min. AD, kontrolery domen oraz lokalne konta na komputerach.<br>• System zdalnego zarządzania powinien umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu poczty elektronicznej lub wiadomości SMS.<br>• System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów na urządzeniach mobilnych wybranych użytkowników.<br>• System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów iOS MDM na urządzeniach mobilnych wybranych użytkowników.<br>• System zdalnego zarządzania powinien tworzyć repozytorium sprzętu w tym min. komputerów i nośników wymiennych.<br>• Administrator powinien mieć możliwość dopisywania informacji do sprzętu w repozytorium w tym min. numeru ewidencyjnego, numeru seryjnego, producenta, daty zakupu, aktualnego użytkownika.<br>• Administrator powinien mieć możliwość zaznaczenia czy urządzenie jest lub nie jest aktualnie wykorzystywane.<br>• Administrator powinien mieć możliwość oznaczania urządzeń jako firmowe.<br>• System zdalnego zarządzania powinien umożliwić zarządzanie urządzeniami mobilnymi z wykorzystaniem serwerów Exchange ActiveSync i iOS MDM.<br>• Zarządzanie urządzeniami przenośnymi Exchange ActiveSync powinno umożliwiać przypisywanie ustawień do wybranych kont pocztowych. |

| | |
|---|---|
| | Ustawienia powinny obejmować w zależności od systemu operacyjnego przynajmniej synchronizacje poczty, korzystanie z określonych aplikacji, ustawienie hasła użytkownika, szyfrowanie danych.<br>• Zarządzanie urządzeniami przenośnymi iOS MDM powinno umożliwiać przynajmniej dodawanie i zmienianie profili konfiguracji, instalować profile zabezpieczeń, instalować aplikacje na urządzeniu przenośnym, zablokować urządzenie przenośne, zresetować hasło urządzenia lub usunąć z niego wszystkie dane.<br>• W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.<br>• W całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej. |

1. **Zamawiający wymaga:**
   1) Na dostarczone serwery, macierz oraz zestawy komputerowe Wykonawca zapewni co najmniej 5 letni okres gwarancyjny z czasem reakcji 4 godziny, naprawa w miejscu instalacji sprzętu. Wykonawca przedstawi przed podpisaniem umowy do akceptacji Zamawiającemu, dokument wystawiony przez producenta oferowanych komputerów (lub jego autoryzowanego przedstawiciela), potwierdzający, że oferowane serwery, będą objęte gwarancją na zasadach określonych w § 6 ust. 2-4 wzoru umowy,
   2) Wykonawca w formularzu ofertowym winien zaznaczyć, które elementy zamówienia będzie powierzał podwykonawcy,
   3) na każdym urządzeniu wchodzącym w przedmiot zamówienia należy zamieścić w widocznym miejscu trwałą nie ścieralną informację wg wzoru:

**„Cyfrowe usługi w zakresie udostępniania informacji publicznej Starostwa Powiatowego w Olecku”**
**UDA-RPWM.03.01.00-28-0006/16-00 w ramach Osi Priorytetowej 3 – „Cyfrowy Region”**
**Działania 03/01/00 – „Cyfrowa dostępność informacji sektora publicznego oraz wysoka jakość e-usług publicznych”**
**Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020**

Wymiary informacji: 12 cm / 6 cm.
Zamawiający wymaga, aby element promocyjny nie odlepiał się po jakimś czasie lub na skutek wykonywania czynności sprzątających typu wytarcie kurzu,

   4) dostarczony sprzęt będzie wolny od wad fizycznych i nie noszący oznak użytkowania. Sprzęt nie może stanowić roszczeń osób trzecich,
   5) zamieszczona powyżej specyfikacja sprzętowa ma wyłącznie charakter przykładowy i dotyczy wymagań minimalnych. Dopuszcza się możliwość zastosowania dowolnych typów i modeli sprzętu pod warunkiem spełniania wyżej określonych parametrów,
   6) w przypadku określenia danego elementu nazwą producenta należy automatycznie stosować pojęcie „lub równoważne”. Równoważność dla poszczególnych elementów (części) jest opisana w poszczególnych tabelach. Równoważność stanowią:
   a) w przypadku systemu operacyjnego dla zestawów Komputerowych oraz Laptopów równoważność jest opisana **w pkt. 3,**
   b) w przypadku pakietu biurowego dla zestawów Komputerowych oraz Laptopów równoważność jest opisana w **pkt. 4,**
   7) w przypadku zaoferowania elementu (części) równoważnego Wykonawca musi podać parametry oferowanego elementu, aby Zamawiający mógł stwierdzić jego równoważność z wymogami SIWZ. Jeżeli równoważny element dotyczy np. rodzaju procesora, który winien

posiadać określoną ilość punktów wskazanych w SIWZ testach, a dla którego to procesora oferowanego przez Wykonawcę nie były prowadzone określone w SIWZ testy rankingowe, Wykonawca musi dołączyć do oferty scenariusz oraz wyniki przeprowadzonych na własny koszt testów oferowanego procesora,

8) ilekroć w opisie przedmiotu zamówienia występują nazwy konkretnych elementów, wyrobów lub określenia (parametry techniczne) sugerujące wyroby, elementy konkretnych firm, producentów Wykonawca winien uznać, iż podano produkty tylko i wyłącznie przykładowe, a Zamawiający dopuszcza możliwość zastosowania elementów, wyrobów, materiałów równoważnych o właściwościach, parametrach technicznych nie gorszych niż przyjęto w szczegółowym opisie przedmiotu zamówienia.

**2. Informacje szczegółowe:**

1) Prace należy realizować w dni robocze w godzinach od 8.00-15.00.
2) Wszystkie prace należy wykonywać w obecności pracownika Zamawiającego.
3) Zakres prac w Starostwie Powiatowym w Olecku:

a) Serwer, macierz, przełączniki:

- montaż serwerów oraz pozostałego sprzętu i oprogramowania w serwerowni w budynku Starostwa Powiatowego w Olecku;
- instalacja, aktualizacja i konfiguracja serwerów w szczegółowym ustaleniu z Zamawiającym i według potrzeb przez niego określonych. Przekazanie licencji;
- oklejenie sprzętu naklejkami promocyjnymi. Wykonanie zdjęć z realizacji zadania,
- przeprowadzenie testów integracyjnych zamontowanego sprzętu;
- przekazanie Zamawiającemu dokumentacji zdjęciowej, licencji, dokumentacji technicznej, nośników, okablowania;
- włączenie, skonfigurowanie wskazanego serwera do urządzenia brzegowego;

b) zestawy komputerowe oraz laptopy:

– dostarczenie sprzętu, wniesienie;
– rozpakowanie sprzętu;
– ułożenie i podłączenie sprzętu we wskazanym miejscu;
– zamaskowanie (ułożenie) okablowania w sposób estetyczny np. w maskownicach;
– instalacja, konfiguracja do potrzeb użytkownika sprzętu komputerowego;
– pobranie aktualizacji systemowych i ich instalacja i konfiguracja;
– wykonanie testów drukowania i połączenia internetowego;
– założenie konta użytkownika i hasła logowania do systemu w uzgodnieniu z użytkownikiem. Hasło i login należy do każdej stacji należy przekazać Zamawiającemu;
– przekazanie kompletu nośników okablowania, licencji;
– oklejenie sprzętu nalepkami promocyjnymi;
– wykonanie zdjęć z zakończonych prac obrazujący sprzęt komputerowy. Na zdjęciach muszą również być widoczne naklejki promocyjne;
– podpisanie protokołu z realizacji instalacji.

4) Wykonawca ustali z Zamawiającym harmonogram prac rozlokowania nowych zestawów.
5) Wykonawca jest zobowiązany do zabrania wszystkich kartonów pochodzących od dostarczonego sprzętu komputerowego. W przypadku potrzeby zgłoszenia sprzętu komputerowego do serwisu Wykonawca będzie w obowiązku dostarczyć do siedziby Zamawiającego oryginalny karton dla danego urządzenia objętego serwisem.
6) Zamawiający zastrzega sobie prawo do weryfikacji oferowanych równoważnych elementów (części) oraz oprogramowania czy spełniają opisy równoważności.
7) W przypadku, kiedy oferowane równoważne elementy lub oprogramowanie nie będą spełniać stawianych warunków oferta zostanie odrzucona jako nie spełniająca warunków SIWZ.
8) W przypadku, kiedy Komisja Przetargowa dojdzie do przekonania, że konieczne będzie

przeprowadzenie weryfikacji ofert równoważnych, to kolejność ich weryfikacji będzie ustalana na podstawie czasu złożenia oferty przetargowej do Zamawiającego.
9) Komisja Przetargowa sporządzi stosowany protokół z przeprowadzonej procedury weryfikującej równoważność zaoferowanych elementów (części) i oprogramowania.

## 3. Opis Równoważności oprogramowania system operacyjny

1) możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek,
2) możliwość dokonywania uaktualnień sterowników urządzeń przez Internet -witrynę producenta systemu,
3) darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) wymagane podanie nazwy strony serwera WWW.
4) internetowa aktualizacja zapewniona w języku polskim,
5) wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6,
6) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
7) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
8) funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
9) interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta,
10) możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu,
11) zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,
12) zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
13) zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych,
14) system operacyjny posiada podstawowe funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika,
15) system operacyjny posiada wbudowaną funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika,
16) zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,
17) wbudowany system pomocy w języku polskim,
18) system operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),
19) możliwość zarządzania stacją roboczą poprzez polityki -przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
20) wdrażanie IPSEC oparte na politykach -wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
21) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
22) wsparcie dla logowania przy pomocy smartcard,
23) rozbudowane polityki bezpieczeństwa -polityki dla systemu operacyjnego i dla wskazanych aplikacji,
24) system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,

25) wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 -możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
26) wsparcie dla JScript i VBScript -możliwość uruchamiania interpretera poleceń,
27) zdalna pomoc i współdzielenie aplikacji -możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; Graficzne środowisko instalacji konfiguracji,
28) rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
29) rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
30) graficzne środowisko instalacji i konfiguracji,
31) transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
32) zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
33) oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
34) możliwość przywracania plików systemowych,
35) system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
36) możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (przy użyciu numerów identyfikacyjnych sprzętu),
37) możliwość podłączenia oraz pełnej integracji z domeną Windows Server 2012R2,
38) obsługa wszystkich zasad grupy Active Directory bez instalacji i konfiguracji dodatkowego oprogramowania.

## 4. Opis Równoważności oprogramowania pakiet biurowy

1) oprogramowanie winno być dostarczone z bezterminową licencją na użytkowanie,
2) wymagania odnośnie interfejsu użytkownika:
   a) pełna polska wersja językowa interfejsu użytkownika,
   b) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych,
   3) pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) edytor tekstów,
   b) arkusz kalkulacyjny,
   c) narzędzie do przygotowywania i prowadzenia prezentacji,
   d) narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
   4) edytor tekstów musi umożliwiać:
   a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
   b) wstawianie oraz formatowanie tabel,
   c) wstawianie oraz formatowanie obiektów graficznych,
   d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
   e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
   f) automatyczne tworzenie spisów treści,
   g) formatowanie nagłówków i stopek stron,
   h) sprawdzanie pisowni w języku polskim,
   i) śledzenie zmian wprowadzonych przez użytkowników,
   j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
   k) określenie układu strony (pionowa/pozioma),

l) wydruk dokumentów,
m) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego,
n) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,
o) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
p) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem,
q) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

5) arkusz kalkulacyjny musi umożliwiać:
a) tworzenie raportów tabelarycznych,
b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),
e) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
f) wyszukiwanie i zamianę danych,
g) wykonywanie analiz danych przy użyciu formatowania warunkowego,
h) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
j) formatowanie czasu, daty i wartości finansowych z polskim formatem,
k) zapis wielu arkuszy kalkulacyjnych w jednym pliku,
l) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
m) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

6) narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a) przygotowywanie prezentacji multimedialnych, które będą prezentowanie przy użyciu projektora multimedialnego,
b) drukowanie w formacie umożliwiającym robienie notatek,
c) zapisanie jako prezentacja tylko do odczytu,
d) nagrywanie narracji i dołączanie jej do prezentacji,
e) opatrywanie slajdów notatkami dla prezentera,
f) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
g) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
h) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
i) możliwość tworzenia animacji obiektów i całych slajdów,
j) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
k) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS

PowerPoint 2003, MS PowerPoint 2007 i 2010.

7) narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
   a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
   b) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
   c) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
   d) automatyczne grupowanie poczty o tym samym tytule,
   e) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
   f) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia,
   g) zarządzanie kalendarzem
   h) udostępnianie kalendarza innym użytkownikom,
   i) przeglądanie kalendarza innych użytkowników,
   j) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
   k) zarządzanie listą zadań,
   l) zlecanie zadań innym użytkownikom,
   m) zarządzanie listą kontaktów,
   n) udostępnianie listy kontaktów innym użytkownikom,
   o) przeglądanie listy kontaktów innych użytkowników,
   p) możliwość przesyłania kontaktów innym użytkowników.