

MINIMALNE WYMAGANIA DOTYCZĄCE SPRZĘTU I OPROGRAMOWANIA KOMPUTEROWEGO

Ocena spełnienia warunków wymaganych od Wykonawcy zostanie dokonana według formuły: spełnia – nie spełnia. W kolumnie „Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego” w poniższych tabelach należy podać parametry oferowanego sprzętu, które pozwolą Zamawiającemu na weryfikację spełnianie wymagań Zamawiającego oraz producenta i model.

Wymagania formalne:

- Urządzenia muszą być fabrycznie nowe i wyprodukowane po 01/01/2017
- Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub normą równoważną.
- W momencie oferowania wszystkie elementy oferowanej architektury muszą być dostępne (dostarczane) przez producenta.
- Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
- Do każdego urządzenia dostarczonego wraz z systemem operacyjnym muszą być załączone oryginalne dokumenty licencyjne (dopuszczalna wersja elektroniczna) uprawniające do używania systemu operacyjnego.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.
- Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu.
- Wszystkie serwery muszą posiadać Certyfikat „B” (dla obudowy) lub oznakowanie CE produktu albo spełniać normy równoważne – nie gorsze niż wymagane przez Zamawiającego.

Wykonawca na etapie wdrożenia musi przedłożyć Deklarację Zgodności z Dyrektywami 72/23/EEC oraz 89/336/EEC (oznaczenie CE) dla serwerów, zasilaczy UPS, komputerów. Wykonawca może zamiast wyżej wymienionego dokumentu - złożyć równoważne zaświadczenie wystawione przez podmioty mające siedzibę w innym państwie członkowskim Europejskiego Obszaru Gospodarczego lub złożyć inne dokumenty potwierdzające odpowiednio stosowanie przez wykonawcę równoważnych środków zapewniania jakości i stosowanie równoważnych środków zarządzania środowiskiem

Dostarczony sprzęt i akcesoria mają po zainstalowaniu i wdrożeniu stanowić spójną całość.

Zasilacz awaryjny UPS (Serwerownia 1 i 2) – 2szt szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Technologia	VFI (true on-line, podwójne przetwarzanie energii)	
	Budowa	Rack 19" 2U	
3	Moc znamionowa	3 kVA / 2,7 kW	
4	Wyjściowy współczynnik mocy (PF)	0,9	
5	Napięcie wejściowe	230 Vac	
6	Sposób zasilania	Plug&Play Gniazdo w standardzie IEC 320	

		W komplecie powinien znajdować się przewód zasilający.	
7	Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie	160 – 276 Vac	
8	Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie	120 – 276 Vac	
9	Częstotliwość wejściowa	40-70 Hz	
10	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 92%	
11	Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%	
12	Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.	
13	Napięcie wyjściowe	230 Vac W komplecie powinny znajdować się przynajmniej 2 przewody odbiorcze.	
14	Częstotliwość wyjściowa	50/60Hz (programowalna) z funkcją autosensing	
15	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)	Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny – wymuszanie opcji Bypass z poziomu panelu LCD	
16	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane	
17	Baterie wewnętrzne	Minimum 6 x 9Ah/12V. Autonomia min. 15 minut przy obciążeniu 1kW.	
18	Zabezpieczenie baterii przed głębokim rozładowaniem	UPS musi być wyposażony w układ chroniący przed głębokim rozładowaniem baterii – napięcie odcięcia baterii powinno być zależne od poziomu obciążenia zasilacza. Opisać poziomy napięcia przy których następuje odcięcie baterii w zależności od poziomu obciążenia.	
19	Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 5-6 lat, <u>umieszczone wewnątrz</u> zasilacza UPS.	
20	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%	
21	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%	
22	Stabilność częstotliwości wyjściowej:	bez synchronizacji: ± 0,05 Hz	
23	Współczynnik szczytu	3:1	
24	Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną	Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości a także napięcia i pozostałej autonomii pracy z baterii podczas gdy UPS pracuje w trybie bateryjnym.	

25	Złącze interfejsów	RS232, USB, programowane złącze REPO do zdalnego wyłącznika pożarowego NO lub NC. Przynajmniej jeden programowany sygnał wyjściowy typu Dry Contact z sygnałem Low Battery.	
26	Gniazda wyjściowe IEC320 na zasilaczu UPS z możliwością zarządzania	Wymagane minimum gniazd – 2 grupy gniazd, w każdej przynajmniej 4 gniazda w standardzie IEC 320-C13. Każda grupa zarządzana z poziomu oprogramowania, z możliwością zdalnego włączenia oraz wyłączenia zasilania danej grupy gniazd. Jedno gniazdo w standardzie IEC 320-C19.	
27	Zdalne wyłączanie dowolnej grupy gniazd podczas pracy normalnej	UPS musi umożliwiać zdalne wyłączenie dowolnej grupy gniazd.	
28	Zdalne wyłączenie dowolnej grupy gniazd po zadanim czasie, gdy UPS przejdzie w tryb pracy z baterii.	W momencie przejścia do pracy baterijnej, UPS musi mieć możliwość automatycznego odłączenia jednej grupy gniazd (część odbiorów) po dowolnie ustawionym czasie 1-30 minut.	
29	Karta sieciowa SNMP	SNMP z protokołem IP v. 4 i 6, obsługą firmware oraz ModBus TCP.	
30	Interfejs EPO (do wyłącznika ppoż.)	Wymagane – styk programowany NO lub NC	
31	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS	
32	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane	
33	Poziom hałasu w odległości 1m,	< 48 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury	
34	Możliwość regulacji z oprogramowania tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane	
35	Zasilacz musi posiadać możliwość upgrade'u wersji oprogramowania sterującego pracą zasilacza.	Wymagane	
36	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane	
37	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane	
38	Wymiary zasilacza UPS w szafie rack z bateriami wewnętrznymi	Maks 2U. Dopuszczalna głębokość UPS 65cm	
38	Waga zasilacza kg	<30 kg	
40	Komplet szyn montażowych Rack	Wymagane	
41	Instrukcja w języku polskim	Wymagane	
42	Gwarancja	36 miesiące	

Przełączniki do serwerowni – 2 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Wymagania podstawowe	Przełącznik posiadający 48 porty 10/100/1000BASE-T Przełącznik posiadający 8 portów 1GBE SFP Możliwość rozbudowy o 4 porty 10 GBE SFP+ Wysokość urządzenia 1U Nieblokująca architektura o wydajności przełączania min. 176 Gb/s Szybkość przełączania min. 130 Milionów pakietów na sekundę Posiada porty umożliwiające łączenie przełączników w stos. Wydajność połączenia w stos min. 40 Gb/s. Możliwość łączenia do 8 przełączników w stos Tablica MAC adresów min. 16k Pamięć operacyjna: min. 1 GB pamięci DRAM Pamięć flash: min. 4 GB pamięci Flash Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094 Obsługa sieci wirtualnych protokołowych IEEE 802.1v Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) Obsługa Q-in-Q IEEE 802.1ad Obsługa Quality of Service IEEE 802.1p DiffServ 8 kolejek priorytetów na każdym porcie wyjściowym Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB Obsługa LLDP Media Endpoint Discovery (LLDP-MED) Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania Wbudowany DHCP Serwer i klient Możliwość instalacji min. dwóch wersji oprogramowania - firmware Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash Możliwość monitorowania zajętości CPU Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring) Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management. Obsługa CDPv2	
2	Obsługa Routingu IPv4	Sprzętowa obsługa routingu IPv4 – forwarding Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów Routing statyczny Obsługa routingu dynamicznego IPv4 RIPv1/v2 OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania	

3	Obsługa Routingu IPv6	Sprzętowa obsługa routingu IPv6 – forwarding Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów Routing statyczny Obsługa routingu dynamicznego dla IPv6 RIPng OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania Telnet Serwer/Klient dla IPv6 SSH2 Serwer/Klient dla IPv6 Ping dla IPv6 Tracert dla IPv6 Obsługa MLDv1 (Multicast Listener Discovery version 1)	
4	Obsługa Multicastów	Filtrowanie IGMP Obsługa Multicast VLAN Registration - MVR Obsługa IGMP v1/v2/v3 snooping	
5	Bezpieczeństwo	Obsługa Network Login IEEE 802.1x - RFC 3580 Web-based Network Login MAC based Network Login Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants) Możliwość integracji funkcjonalności Network Login z Microsoft NAP Przydział sieci VLAN, ACL/QoS podczas logowania Network Login Obsługa Guest VLAN dla IEEE 802.1x Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication Obsługa Identity Management Wbudowana obrona procesora urządzenia przed atakami DoS Obsługa TACACS+ (RFC 1492) Obsługa RADIUS Authentication (RFC 2138) Obsługa RADIUS Accounting (RFC 2139) RADIUS and TACACS+ per-command Authentication Bezpieczeństwo MAC adresów ograniczenie liczby MAC adresów na porcie zatrzaśnięcie MAC adresu na porcie możliwość wpisania statycznych MAC adresów na port/vlan Możliwość wyłączenia MAC learning Obsługa SNMPv1/v2/v3 Klient SSH2 Zabezpieczenie przełącznika przed atakami DoS Networks Ingress Filtering RFC 2267 SYN Attack Protection Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 Adres MAC źródłowy i docelowy plus maska Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6 Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd. Numery portów źródłowych i docelowych TCP, UDP	

		Zakresy portów źródłowych i docelowych TCP, UDP Identyfikator sieci VLAN - VLAN ID Flagi TCP Obsługa fragmentów Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania Obsługa bezpiecznego transferu plików SCP/SFTP Obsługa DHCP Option 82 Obsługa IP Security - Gratuitous ARP Protection Obsługa IP Security - Trusted DHCP Server Obsługa IP Security - DHCP Snooping Obsługa IP Security - DHCP Secured ARP/ARP Validation Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s	
6	Bezpieczeństwo sieciowe	Możliwość konfiguracji portu głównego i zapasowego Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania Obsługa STP (Spanning Tree Protocol) IEEE 802.1D Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s Obsługa PVST+ Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619 Obsługa G.8032 v1/v2 Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.	
7	Zarządzanie	Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol) Obsługa synchronizacji czasu NTP Zarządzanie przez SNMP v1/v2/v3 Zarządzanie przez przeglądarkę WWW – protokoły http i https Możliwość zarządzania poprzez protokół XML Telnet Serwer/Klient dla IPv4 / IPv6 SSH2 Serwer/Klient dla IPv4 / IPv6 Ping dla IPv4 / IPv6 Traceroute dla IPv4 / IPv6 Obsługa SYSLOG z możliwością definiowania wielu serwerów Sprzętowa obsługa sFlow Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757) Obsługa RMON2 (RFC 2021)	
8	Inne	Zakres temperatury pracy 0-50 °C Obsługa skryptów CLI	

		Obsługa funkcji TCL/Tk w skryptach CLI Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) Obsługa OpenFlow – możliwość rozszerzenia przez licencje Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje Możliwość uruchamiania skryptów Ręcznie O określonym czasie lub co wskazany okres czasu Na podstawie wpisów w logu systemowym	
9	Gwarncja	36 miesięcy	

Wypożyczenie serwerowni - 2 kpl

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Szafa	Możliwość kontrolowania drogi przepływu powietrza poprzez zastosowanie odpowiedniego rodzaju drzwi, osłon bocznych i tylnej oraz paneli wentylacyjnych. Rama spawana z profili stalowych gr. 1,5 mm, przystosowana do ustawienia na nóżkach poziomujących lub montowana na cokole. Obrzeże dachu perforowane dla bardziej wydolnej wentylacji szafy. W dachu i podstawie po dwa otwory 8U pod zainstalowanie paneli wentylacyjnych oraz po dwa otwory 2U szer. min 450 mm do wprowadzenia kabli. Dodatkowe otwory 2U szer. min 450 mm. Wszystkie otwory występujące w ramie zaślepienie na mikrołączach i są wyłamywane według potrzeby użytkownika Możliwość zastosowania kompletu kół jezdnych. Przy zastosowaniu kółek maksymalna nośność szaf statycznie (nie licząc masy szafy) nie może przekraczać 150 kg. Drzwi przednie jednoskrzydłowe pełne szkło z możliwością montażu prawo i lewostronnego z zamkiem trzypunktowym z klamką, zamontowane na zawiasach umożliwiających otwarcie drzwi o 180°. Ściany boczne z blachy stalowej gr. 1 mm, zdejmowane Cztery pionowe profile montażowe 19" z blachy ocynkowanej (numerowane co 1U) montowane do kątowników w dachu i podłodze szafy (co skutecznie zwiększa jej nośność), tworzy trzy płaszczyzny montażowe. Listwa zasilająca z zabezpieczeniem przeciwprzepięciowym do montażu w szafie 19"- 2 szt Rozstaw profili montażowych to odpowiednio dla głębokości szaf (max):	
2	Panel wentylacyjny do szafy	Montowany w dachu i podstawie proponowanej szafy	

3	patchpanel	48-portowy patch panel ekranowany kategorii 6 do szafy 19". Wysokość 1U. Złącza typu Dual Block Każdy z portów oznaczony jest diodą, która pozwala na łatwą identyfikację toru kablowego i weryfikację poprawności jego zakończeń.	
4	Konsola KVM	• Monitor LCD min 15" • Możliwość podłączenia min 6 urządzeń • Zamykana i chowana w szafie • Klawiatura • Mysz lub track ball	

Serwer bazy danych, serwer plików, dostępowy – 3 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Obudowa	Obudowa o wysokości maksymalnie 1U, dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.	
2	Typ procesora	Procesor wielordzeniowy dedykowany do pracy w serwerach wieloprocessorowych.	
3	Wydajność procesora	Wydajność procesora na stronie https://www.cpubenchmark.net/multi_cpu.html musi osiągnąć min. 16933 punktów	
4	Ilość procesorów	Zainstalowane 2 procesory.	
5	Pamięć RAM	Zainstalowane 128GB pamięci operacyjnej DDR4 z korekcją błędów ECC. Minimalna wielkość pojedynczej kości pamięci musi wynosić 16 GB Możliwość rozszerzenia pamięci do minimum 1200GB.	
6	Płyta główna	Dwuprocessorowa, dedykowana do pracy w serwerach, wyprodukowana przez producenta procesora.	
7	Sloty PCI	Minimum 2 sloty PCI-E x8.	
8	Dyski HDD	8 szt dysków SSD 2.5" o pojemności co najmniej 480Gb klasy serwerowej	
9	Kontroler macierzowy	Karta SAS 12 Gb/s wyposażona w minimum 2 porty wewnętrzne. Wymagane potrzebne okablowanie	
10	Karta rozszerzeń	Zintegrowane z płytą główną 2 porty sieciowe Gigabit Ethernet. Możliwość uruchomienia 2 portów 10Gb/s, do których dostęp aktywowany jest poprzez instalację dodatkowej karty rozszerzeń, niezajmującej żadnego ze slotów PCI-E, lecz posiadającej swoje dedykowane złącze na płycie głównej.	
11	Karta graficzna	Zintegrowana karta graficzna 16MB	
12	Porty	2 porty RJ-45. 1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania. 5 portów USB 3.0 (2 z przodu, 3 z tyłu) 2 porty VGA .	

13	Napęd dysków optycznych	Wewnętrzny DVD-RW.	
14	Zasilanie	Redundantne zasilacze typu Hot-Plug, minimalna moc 750W na zasilacz. I sprawności 80 plus platynium mogące pracować w przy zasilaniu 120V lub 230V	
15	Chłodzenie	Redundantne podwójne wiatraki typu Hot-Plug.	
16	Bezpieczeństwo	Panel diagnostyczny dostępny od frontu serwera, podający informacje o statusie serwera, wyświetlający informacje o błędach, Serwer musi umożliwiać przewidywanie awarii, i na tej podstawie wymianę wadliwych części przed wystąpieniem awarii.	
17	Zgodność	Serwer musi posiadać certyfikacje z systemami Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 VMware	
18	Certyfikaty	Serwer musi posiadać certyfikac CE oraz ISO 9001	
19	Urządzenia dodatkowe	Serwer musi być wyposażony w klawiaturę i mysz podłączaną za pomocą USB w układzie US, trwale oznaczone logiem producenta Serwera.	
20	Serwis	Serwis świadczony na miejscu instalacji z czasem reakcji serwisu w ciągu jednej godziny, i naprawy w ciągu do 2 dni roboczych, Zamawiający dopuszcza rozszerzenie gwarancji na o kolejne lata, proszę o przedstawienie kalkulacji na kolejne 2lata, i 3 lata ponad standardowe 3 lata serwisu. Serwis musi być świadczony przez certyfikowanego partnera producenta serwera. Oferent w celu zapewnienia jak najlepszej znajomości rozwiązania musi posiadać certyfikacje serwisową producenta.	
21	Pochodzenie	Serwer musi pochodzić z oficjalnego kanału producenta, i być wyprodukowany nie wcześniej jak w dniu otwarcia ofert przez zamawiającego.	
22	Czas dostawy	Zamawiający wymaga dostarczenia sprzętu w terminie nie przekraczającym 3 tygodnie od podpisania zamówienia.	
23	System operacyjny	- Serwery powinny być dostarczone z systemem operacyjnym w najnowszej wersji - System powinien umożliwiać uruchomienie usługi katalogowej zgodnej MS AD - System powinien w pełni wspierać dostarczany serwer - Sytem powinien wspierać konfiguracje tzw. Site and Services - System powinien umożliwiać konfiguracje funkcjonalności DFS - System powinien umożliwiać konfigurację Network Policy Server dla portokołu 802.1x skonfigurowanego na przełącznikach	

Licencje dodatkowe

LP	Licencja	sztuk	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Dostęp usług oferowanego systemu operacyjnego dla serwerów	40	
	Licencja umożliwiająca dostęp do usług terminala zdalnego dla oferowanego systemu operacyjnego dla serwerów	4	

Stanowiska mobilne – 10 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1		Przekątna ekranu 15,6 cali	
2	Matryca	Matryca zapobiegająca odbłaskom Nominalna rozdzielczość 1920 x 1080 pikseli	
3	Procesor	Procesor: osiągający co najmniej 4711 punktów w teście Passmark CPU Mark publikowany na stronie https://www.cpubenchmark.net/cpu_list.php , oraz charakteryzujący się współczynnikiem TDP nie większym niż 15W.	
4	Pamięć	Pamięć: co najmniej 4GB z możliwością rozszerzenia do 32GB	
5	Dysk	Pojemność dysku twardego nie mniejsza niż 240 GB osiągającego prędkość zapisu co najmniej 515MB/s oraz prędkość odczytu 530MB/s, z możliwością zainstalowania 2 dysku twardego	
6	Napęd	Napęd optyczny DVD+/-RW	
7	Karta graficzna	Karta graficzna osiągająca co najmniej 945 punktów w teście PassMark GPU publikowanego na stronie http://www.videocardbenchmark.net/mid_range_gpus.html	
8	Karta dźwiękowa	Karta dźwiękowa: wejście mikrofonu, dwa wbudowane głośniki, wyjście liniowe,	
9	Czytnik kart	Czytnik kart pamięci obsługujący karty SD/MMC/RSMMC/SDHC/SDXC/MiniSD	
10	Komunikacja	Komunikacja * Moduł wi fi mogący pracować w zakresach Wi-Fi 802.11 a/b/g/n/ac * LAN 100 Mbps * Bluetooth 4.0	

11	Klawiatura	Klawiatura w układzie US podświetlana z wydzieloną klawiaturą numeryczną	
12	Interfejsy	Interfejsy: oznaczenie interfejsów na powierzchni wewnętrznej(tam gdzie jest klawiatura) w celu łatwego identyfikowania portów oraz na krawędziach bocznych. *2 x USB 2.0 *1 x USB 3.0 *1 x USB 3.0 typ C *1 x RJ45 *1 x HDMI *1 x VGA (D-Sub) *1 x zapięcie Kensington	
13	Inne	Waga urządzenia nie może przewyższyć 2.2kg Bateria Litowo Jonowa z możliwością wymiany bez konieczności otwarcia obudowy o pojemności nie mniejszej niż 44Wh Możliwość dołożenia modelu LTE wewnętrznego.	
14	Gwarancja	Gwarancja 3 lata z serwisem odbioru sprzętu w razie awarii i dostarczeniem go po naprawie do siedziby zamawiającego	

Stanowiska komputerowe – 30 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Procesor	Procesor klasy x86 musi osiągać w teście wydajności PassMark Performance. Test co najmniej wynik 6688 punktów Passmark CPU Mark. Wynik dla oferowanego procesora na dzień ukazania się postępowania lub późniejszy powinien być opublikowany na stronie: https://www.cpubenchmark.net/cpu_list.php	
2	Pamięć	Pamięć operacyjna RAM co najmniej 4GB w technologii DDR4 non-ECC możliwość rozbudowy do 32GB.	
3	Dysk	Parametry pamięci masowej Dysk twardy o pojemności przynajmniej 500 GB ze złączem SATA III i prędkość obrotowej 7200rpm posiadającej co najmniej 32MB cache	
4	Dodatkowe porty	Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.	
5	Obudowa	- Obudowa Typu MiniTower suma wymiarów obudowy nie może przekraczać 945mm - Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami	
6	Dodatkowe wymagania	Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie	
7		- System (64-bit), umożliwiający współpracę z Active Directory w pełny sposób obsługujący wszelkie funkcjonalności domeny w wersji 2016 - zainstalowany system operacyjny nie wymagający aktywacji za pomocą telefonu ani Internetu	
8	Nagrywarka	Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt	
9	Klawiatura	- Dołączona klawiatura w układzie US oraz mysz trwale oznaczona logiem producenta komputera. - Sterowniki do pobrania ze strony producenta po podaniu nr seryjnego	
10		Dołączona klawiatura w układzie US oraz mysz trwale oznaczona logiem producenta komputera.	
11	sterowniki	Sterowniki do pobrania ze strony producenta po podaniu nr	

		seryjnego	
12	Certyfikaty i Standardy	- Deklaracja zgodności CE dla oferowanego komputera; - Komputer musi spełniać wymogi normy Energy Star. - Potwierdzeniem jest certyfikat poświadczony przez producenta	
13	Gwarancje	3-letnia gwarancja producenta świadczona na miejscu u klienta, - W przypadku awarii dysków twardych dyski pozostają u Zamawiającego. - Czas reakcji serwisu – w ciągu jednej godziny. - usługi serwisowe świadczone w miejscu instalacji urządzenia - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu - przez cały rok (w języku polskim w dni robocze), - szybkie wsparcie telefoniczne świadczone przez wyszkolonych inżynierów,, - w przypadku wystąpienia usterki wymagana jest natychmiastowa reakcja wsparcia technicznego (diagnostyka zaraz po wystąpieniu awarii). - Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
14	Monitor	- Monitor TFT z podświetleniem w technologii LED - Proporcje obrazu: 16:9, - Przekątna ekranu co najmniej 24", Typ matrycy TFT- TN - Plamka matrycy max: 0.277 mm, - Rozdzielczość min 1920 x 1080, - Czas reakcji max: 5ms - Czas reakcji z Szarości do szarości max: 2ms - Jasność min: 250 cd/m², - Kontrast dynamiczny 20 000 000:1, - Kąt widzenia poziom/pion 170 °/160 °, - Ilość kolorów 16,7 mln, - Gniazda we/wy 1 x 3,5 mm minijack , 1 x 15-pin D-Sub, 1x DVI-D, - Możliwość pochylania monitora do przodu co najmniej 5st, do tyłu co najmniej 20st. - Otwory montażowe w standardzie Vesa 100mm - Zintegrowane głośniki - Monitor w trybie czuwania nie może pobierać więcej jak 0,5Watt energii, - Monitor w trybie pracy nie może pobierać więcej jak 19 W energii, - W zestawie z monitorem musi być załączony kabel do podłączenia zasilania, audio, oraz obrazu w standardzie cyfrowym. - Waga monitora wraz ze stopką nie może przekroczyć 3.6kg - Monitor musi posiadać certyfikat CE, EN 60950, oraz być zgodny z EnergyStar - Gwarancja 2 lata z serwisem odbioru sprzęt w razie awarii i dostarczeniem go po naprawie do siedziby zamawiającego. Gwarancja będzie obejmować w trakcie trwania uszkodzenie polegające na wadliwym bądź braku działania nawet jednego piksela.	

UPS dla stanowisk komputerowych

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Moc pozorna	800 VA	
2	Moc rzeczywista	480 Wat	
3	Architektura UPSa	line-interactive	
4	Maks. czas przełączenia na baterie	6 ms	
5	Liczba i rodzaj gniazdek z utrzymaniem zasilania	2 x PL (10A)	
6	Typ gniazda wejściowego	IEC320 C14 (10A)	
7	Czas podtrzymania dla obciążenia 100%	1 min	
8	Czas podtrzymania przy obciążeniu 50%	5 min	
9	Zakres napięcia wejściowego w trybie podstawowym	220-240 V	
10	Zmienny zakres napięcia wejściowego	170-280 V	
11	Zimny start	Tak	
12	Diody sygnalizacyjne	- praca z sieci zasilającej - praca z baterii - znaczące wyczerpanie baterii	
13	Alarmy dźwiękowe	- praca z baterii - awaria sieci zasilającej - znaczące wyczerpanie baterii	
14	Typ obudowy	- Desktop - Kompaktowe rozmiary	
15	Wyposażenie	- Instrukcja obsługi - Kabel zasilający - Kabel do podłączenia komputera	
16	Dodatkowe informacje	- Czas ładowania baterii 4h - 90% - Automatyczny restart po powrocie zasilania - Symulowana sinusoida podczas pracy na baterii - Możliwość montażu na ścianie	

Drukarka laserowa do stanowisk komputerowych – 26 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające

			spełnienie wymagań Zamawiającego
1	Szybkość drukowania w A4	40 str./min w mono	
2	Czas pierwszego wydruku	do 5 sekund	
3	Rozdzielczość	1200 x 1200 dpi	
4	Języki druku	PCL5e, PCL6, Epson FX, IBM Pro-Printer, XPS, PDF (v1.7), PostScript 3 emulacja	
5	Czcionki drukarki	80 skalowanych czcionek PCL i 130 czcionek PostScript	
6	Zespół drukowania	Dupleks mechaniczny	
7	Złącza	Port USB 2.0, Ethernet 10/100/1000BaseTX, Urządzenie musi posiadać możliwość instalacji karty sieciowej bezprzewodowej WLAN802.11a/b/g/n	
8	Kompatybilność z systemami operacyjnymi	Windows 7 (32-bitowy i 64-bitowy), Windows 8 (32-bitowy i 64-bitowy), Windows 8.1 (32-bitowy i 64-bitowy), Windows Server 2003 (32-bitowy i 64-bitowy), Windows Vista (32-bitowy i 64-bitowy), Windows Server 2008 (32-bitowy i 64-bitowy), Windows Server 2008 R2 (64-bitowy), Windows Server 2012 (64-bitowy), Windows Server 2012 R2 (wersja 32-bitowa i 64-bitowa); Linux PPD; Mac OS 10.6.8-10.7, 10.8, 10.9	
9	Dodatkowe oprogramowanie	Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - funkcjonować w środowisku Windows; - obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT) - podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; - możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; - podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów); - możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.	
10	Pojemność papieru	Podajnik 1: 250 arkuszy 80 g/m ² ; Podajnik uniwersalny: 100 arkuszy 80 g/m ² ; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m ²	
11	Format papieru	Podajnik 1: A4, A5, B5, A6 Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, nośniki (baner) do 120 cm długości Druk dwustronny: A4, B5	
12	Gramatura papieru	Podajnik 1: 60 – 120 g/m ² ; Druk dwustronny: 60 – 120 g/m ² ; Podajnik uniwersalny: 60 – 163 g/m ²	
13	Odbiornik papieru	Do 150 arkuszy stroną zadrukowaną do dołu	

		Do 100 arkuszy stroną zadrukowaną do góry	
14	Wymaganie dodatkowe:	Płaski przebieg przy materiałach o dużej gramaturze	
15	Pamięć (RAM)	Standardowa pamięć RAM: 512MB	
16	Szybkość procesora	660 MHz	
17	Obciążenie	Maksymalne obciążenie do 80 000 stron miesięcznie	
18	Gwarancja	3 lata gwarancji producenta drukarki - naprawa w autoryzowanym serwisie ciągu 72h od daty dostarczenia urządzenia.	
19	Materiały eksploatacyjne:	Wymagana rozdzielność bębna i tonera.	

Drukarka przenośna z baterią – 5 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Standardowa pamięć [MB]	128	
2	Normatywny cykl pracy (miesięcznie, format A4) [arkusz]:	500	
3	Zalecana ilość miesięczna [str./m-c]:	100-300	
4	Technologia druku:	Atrament - kolor	
5	Format druku	A4	
6	Szybkość drukowania - mono [str. / min.]:	18	
7	Szybkość drukowania - kolor [str. / min.]:	17	
8	Rozdzielczość druku - mono [dpi]:	1200x1200	
9	Rozdzielczość druku - kolor [dpi]:	4800 x 1200	
10	Czas wydruku 1-wszej strony [sek.]:	12	
11	Ilość wkładów	<u>2 (1x czarny, 1x kolorowy)</u>	
12	Interfejsy komunikacyjne	<u>WiFi (drukowanie bezprzewodowe, wireless) , USB 2.0</u>	
13	Obsługiwane formaty nośników:	<u>A4, A5, A6, B5 (ISO), B5 (JIS); Koperty (A2, C5, C6, DL); Papier fotograficzny (10 × 15 cm)</u>	
14	Zużycie energii [W]:	<u>15 W (aktywność), 0,17 W (urządzenie wyłączone ręcznie), 3,9 W (tryb czuwania), 1,14 W (tryb uśpienia)</u>	
15	Standardowe języki drukarki:	<u>PCL 3</u>	
16	Bateria	Możliwość pracy bez podłączenia do sieci zasilania	

Urządzenie wielofunkcyjne A3 – 3 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
	Pamięć systemowa	128	
	Protokoły sieciowe	TCP/IP (IPv4; IPv6); HTTP; SNMP	
	Automatyczny podajnik dokumentów	do 70 oryginałów; podajnik A5-A3	
	Format papieru	A5-A3	
	Własne formaty papieru	90–297 x 140–432 mm	
	Pojemność Standard: wejściowa papieru	Standard: 350 arkuszy, Maks. 1 350 arkuszy	
	Podajnik boczny papieru	100 arkuszy; A5-A3; Własne formaty papieru (90-297 x 140-432 mm); 64-157 g/m2	
	Opcje wykańczania	Grupowania, sortowanie, krzyżowe	
	Pojemność odbiorcza	min.: 250 arkuszy	
	Wolumen kopii/druku miesięcznie	Zalecany: 5 000 stron	
	Wydajność tonera	12000 stron	
	Pobór mocy	220-240 V/50/60 Hz, poniżej 1,3 kW	
	Waga urządzenia	Maks 30Kg	
	Proces kopiowania	Laserowy elektrostatyczny transfer obrazu	
	Szybkość kopiowania/ druk A4	22 str/min	
	Szybkość kopiowania/ A3	8 str /min	
	Czas oczekiwania na pierwszą kopie	Do 6,5 sek	
	Czas przygotowanie do pracy	Do 15 sek	
	Rozdzielczość kopiowania	600x600 dpi	
	Półtony	256 odcieni	
	Format oryginału kopiowania	A5-A3	
	Powiększenie	25-400% w odstępach co 0.1%	
	Funkcje kopiowania	2 na 2, 4 na 1, kopiowanie książki, dokumentów identyfikacyjnych, przesunięcie marginesu, usuwanie obracanie obrazu, rejestrowanie programu	
	Szybkość skanowania	Mono 46 /min – kolor 20/min	
	Rozdzielczość skanowania	600x600dpi	
	Tryby skanowania	skanowanie do e-mail (opcja) skanowanie do SMB (opcja) skanowanie do FTP (opcja) skanowanie do USB skanowanie lokalne TWAIN	
	Formaty plików	JPEG; TIFF; PDF	
	Miejsca składowania dokumentów	32 ustalone jednym dotykaniem 250 miejsc szybkiego wyboru wsparcie LDAP	
	Transmisja faksu	Analogowa i-Fax	
	Rozdzielczość faksu	Standard; Fine; Super-fine Maks. 408 x 392 dpi	

Kompresja faksu	MH; MR; MMR; JBIG	
Faks modem	Do 33,6 Kbps	
Miejsca docelowe faksów	32 miejsca ustalone jednym dotykaniem 250 miejsc szybkiego wyboru	
Funkcje faksu	PC-Fax, polling, przekazywanie, książka telefoniczna, ponowne wybieranie numeru	
Rozdzielczość druku	GDI: 600 x 600 dpi PCL (opcja:) 1 200 x 600 dpi	
Język opisu strony	GDI	
Wspierane systemy operacyjne	Windows Vista (32/64) Windows 7 (32/64) Windows 8 (32/64) Windows 10 (32/64) Windows Server 2008 (32/64) Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2	
Czcionki drukark	53 PCL Latin	
Funkcje druku	N-up, znak wodny, bezpieczny druk, obracanie obrazu	

Oprogramowanie do backupu – 1 kpl.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	instalator	Instalator powinien umożliwiać zainstalowanie aplikacji klienckiej na komputerze użytkownika końcowego. Instalator powinien posiadać następujące funkcje: • Kreator instalacji, • Automatyczna instalacja dodatkowych komponentów	
2	Aplikacja Windows	Część kliencka powinna składać się z dwóch elementów, aplikacji klienckiej oraz usługi systemowej. Aplikacja kliencka instalowana na komputerze użytkownika końcowego odpowiedzialna za konfigurację i administrację politykami backupu. Usługa systemowa właściwy silnik backupu, odpowiedzialna za wykonywanie backupów oraz synchronizację danych. Aplikacja kliencka nie musi być uruchomiona dla prawidłowego działania usługi.	

	Backup i przywracanie danych	• Deduplikacja danych na źródle, • Backup przyrostowy Delta, • Backup różnicowy Delta, • Bare Metal Recovery, • Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, • Retencja danych • Kreator projektów backupów - polityka backupu, • Projekty backupów, • Backup danych lokalnych - plikowy, • Backup MS Outlook, • Backup MS SQL, • Backup Firebird, • Backup dysków sieciowych, • Backup MS Exchange 2007 , 2010, 2013, • Backup MySQL, • Backup PostgreSQL, • Backup System State, • Backup Hyper-V, • Backup VMware, • Backup VMware dla darmowych licencji, • Windows Operating System Backup – VHD, • Backup z wykorzystaniem skryptów pre i post, • Backup obrazu dysku - Obraz HDD, • Harmonogramy backupów, • Backup otwartych plików (VSS), • Filtr plików oraz folderów, • Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), • Wyłączanie komputera po wykonaniu backupu, • Backup na prawach użytkownika systemu Windows, • Backup na prawach użytkownika AD, • Przywracanie danych do wskazanego katalogu, • Przywracanie danych do pierwotnej lokalizacji, • Przywracanie wybranej wersji pliku, • Możliwość backup-u z wykorzystaniem wielu rdzeni procesora, • Możliwość przywracania z wykorzystaniem wielu rdzeni procesora, • Przywracanie plików z określonego hosta, • Przywracanie plików z określonego projektu, • Przywracanie całych systemów operacyjnych (beta), • Przywracanie Exchange bezpośrednio do serwera. • Przywracanie Hyper-V bezpośrednio do hosta maszyn, • Przywracanie Exchange 2013 na poziomie pojedynczej skrzynki, • Usuwanie plików przesłanych jako backup, • Usuwanie wybranej wersji pliku, • Wyszukiwanie plików w repozytorium użytkownika, • Nadpisywanie plików podczas ich przywracania.	
3	Ustawienia użytkownika	Użytkownik końcowy powinien móc konfigurować zainstalowaną aplikację w następującym zakresie: • Zmiana języka aplikacji, • Automatyczne logowanie, • Zapamiętywanie danych logowania, • Automatyczne uruchamianie programu przy starcie systemu, • Eksport oraz import konfiguracji do pliku, • Eksport oraz import konfiguracji na serwer, • Ograniczenie ilości przechowywanych wersji,	

		● Ustawianie priorytetu dla procesu backupu, ● Zmiana klucza szyfrującego, ● Ustawienia proxy, ● Ustawienia przepustowości/zajętości pasma, ● Konfiguracja wydajności procesu backupu, ● Możliwość ograniczenia obciążenia dysku twardego, ● Możliwość wyłączenia zdalnego zarządzania.	
4	Aktualizacje	● Automatycznie, ● Ręcznie	
3	Bezpieczeństwo	● Zastępowanie nazwy pliku GUID-em, ● Szyfrowanie danych algorytmem AES 256 CBC zawsze po stronie komputera użytkownika, ● Kompresja danych, ● Transmisja po bezpiecznym protokole SSL, ● Deklaracja domyślnego klucza szyfrującego, ● Deklaracja klucza szyfrującego użytkownika, ● Zmiana klucza szyfrującego, ● Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, ● Obliczanie sumy kontrolnej SHA-1,	
4	Obsługiwane języki	● polski ● angielski	
3	Pozostałe	● Shell Menu (menu kontekstowe systemu Windows), ● Kreator pierwszego uruchomienia, ● Rozbudowanie logi aplikacji kliencie oraz usługi, ● Możliwość instalacji samej usługi – do zarządzania przez Management Center, ● Automatycznie wyszukiwanie serwerów backupu w sieci, ● Komunikaty z tray, ● Wskazywanie statusu połączenia z serwerem, ● Mechanizm łatwego raportowania błędów.	
4	Aplikacja CLI	● obsługa backupu plikowego ● Aplikacja zarządzana za pośrednictwem centralnej consoli ● Wbudowana pomoc	
	Aplikacje Serwerowe	System powinien działać w architekturze klient-serwer. System powinien być dowolnie skalowany. ● Bezpośrednia instalacja oprogramowania na serwerze sieciowym NAS (z systemem QTS 4.0) bez potrzeby wstawiania serwera pośredniego ● Magazyn danych jako jednostka logiczna, ● Automatyzacja procesów związanych z uszkodzeniem magazynów ● System sprawdzania integralności i spójności danych, ● Narzędzie do cyklicznego oczyszczenia magazynów ze zbędnych plików, ● Skalowalność oraz niezawodność, ● Platforma jest kompatybilna z Open Stack oraz Amazon (S3 i EC2), ● Współpraca z API NAS'a, na którym oprogramowanie do backupu jest zainstalowane,	
	Centralne zarządzanie	● Zdalne zarządzanie aplikacjami klienckimi, ● Tworzenie i edycja użytkowników, ● Możliwość tworzenia grup i przypisywania użytkowników do wybranej grupy, ● Zdalne tworzenie, na urządzeniach końcowych, projektów backupów podstawowych oraz zaawansowanych, ● Automatycznie wyszukiwanie serwerów backupu w sieci, ● Wyzwalanie backupów na aplikacjach klienckich,	

		• Edycja projektów backupów zapisanych na urządzeniach końcowych, • Przywracanie danych, które zostały poddane backupowi, na dowolne urządzenie, • Przywracanie danych, które zostały poddane backupowi, na komputer administratora, • Zdalna konfiguracja użycia zasobów komputera klienckiego przez aplikację podczas wykonywania backupu, • Przypisywanie urządzeń do kont użytkowników, • Usuwanie urządzeń przypisanych do użytkowników, • Wgląd do dziennika zdarzeń poszczególnych użytkowników platformy, • Zarządzanie magazynami danych, • Grupowanie projektów w szablony, • Zarządzanie szablonami backupów, • Przesyłanie zdefiniowanych szablonów do aplikacji klienckich, • Zarządzanie sesjami backupu, • Integracja z Active Directory – mapowanie użytkowników, • Zdalna i cicha instalacja, • Pobieranie informacji na temat urządzeń użytkowników aplikacji klienckich, • Pobieranie aplikacji klienckich, • Wgląd do logów wszystkich usług platformy, • Możliwość raportowania błędów, • Generowanie raportów oraz wykresów, • Możliwość uruchomienia wykonanego obrazu dysku jako maszynę wirtualną bez konieczności użycia zewnętrznego wirtualizatora • Funkcjonalność Bare Metal Recovery dająca możliwość przywrócenia systemu operacyjnego na nowym sprzęcie (np. nowym laptopie) oraz możliwość bezpośredniego zwirtualizowania backupowanego wcześniej systemu na nowym sprzęcie. Rozwiązanie powinno dostarczać wirtualizator niezbędny do uruchomienia maszyny wirtualnej z obrazu znajdującego się na medium backupowym. • Zarządzanie szablonami backupu, • Monitorowanie sesji, • Wykresy oraz statystyki, • Wskazywanie statusu połączenia z serwerem, • Możliwość definiowania wielu ścieżek jednoczesnego zapisu dla jednego magazynu – redundancja, • Możliwość ręcznego uruchomienia oczyszczenia magazynów ze zbędnych plików, • Archiwizacja danych - możliwość eksportu danych do wersji natywnej i ich zapisów w dowolnej lokalizacji - funkcja realizowana w całości przez serwer, • Możliwość zarządzania magazynami danych, • Kreator pierwszej konfiguracji systemu	
	Wspierane systemy operacyjne dla klienta	• Microsoft Windows od XP wzwyż, • Microsoft Windows Server od 2003 wzwyż, • Unix/Linux, • OS X, • Android, • iOS, • Novell NetWare 6.5.	
5	Storage	Razem z aplikacją backupu powinno być dostarczone urządzenie dyskowe do składowania kopii bezpieczeństwa o pojemności min 12 TB	

		przy zastosowaniu konfiguracji dysków RAID 5 urządzenie powinno mieć możliwość zainstalowania na nim proponowanego oprogramowania backup	
6	Wymagania	Dostarczane oprogramowanie backup powinno umożliwiać backup wszystkich maszyn wirtualnych na 2 serwerach fizycznych, backup bazy danych Postgresql	

Oprogramowanie zabezpieczające – 40 licencji

Producent.....

Model

LP	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10	
2	Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.	
3	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.	
4	Wbudowana technologia do ochrony przed rootkitami.	
5	Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	
6	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	
7	System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.	
8	Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami	
9	Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.	
10	Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).	
11	Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.	
12	Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.	
13	Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.	
14	Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.	
15	Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.	
16	Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).	
17	Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).	
18	Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	
19	Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.	

20	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	
21	Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.	
22	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	
23	Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	
24	Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	
25	Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.	
26	Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	
27	Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.	
28	Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.	
29	Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.	
30	Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.	
31	Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.	
32	Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.	
33	Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.	
34	Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.	
35	Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.	
36	System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.	
37	Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.	
38	Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.	

39	Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.	
40	Program ma być w pełni zgodny z technologią CISCO Network Access Control.	
41	W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.	
42	Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.	
43	Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.	
44	Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.	
45	Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.	
46	Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.	
47	Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.	
48	Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.	
49	Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.	
50	Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.	
51	Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.	
52	Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook.	
53	Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.	
54	Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.	
55	Zapora osobista ma pracować jednym z 4 trybów: - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.	
56	Możliwość tworzenia list sieci zaufanych.	
57	Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie	

58	Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.	
59	Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.	
60	Program musi umożliwić ustalenie tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.	
61	Program musi posiadać kreator, który umożliwi rozwiązać problemy z połączeniem.	
62	Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.	
63	Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.	
64	Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.	
65	Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.	
66	Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.	
67	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.	
68	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	
69	Wbudowana technologia do ochrony przed rootkitami i exploitami.	
70	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	
71	Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux.	
72	Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).	
73	Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.	
74	Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.	
75	Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.	
76	Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.	
77	Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.	
78	Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.	
79	Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.	
80	Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.	
81	Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.	
82	Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.	
83	Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.	

84	Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.	
85	Serwer administracyjny musi być wyposażona w mechanizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.	
86	Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).	

Urządzenie do zabezpieczenia sieci/ochrona przed atakami – 2 szt.

Producent.....

Model

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	System musi wspierać IPv4 oraz IPv6 w zakresie	1. Firewall. 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego.	
2	Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.	
3	Interfejsy, Dyski:	1. System realizujący funkcję Firewall musi dysponować minimum 14 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.	
4	Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps. 4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 2,5 Gbps.	

		5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 300 Mbps	
5	Funkcje Systemu Bezpieczeństwa:	1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Analiza ruchu szyfrowanego protokołem SSL. 10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 11. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.	
6	Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	
7	Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2.	

		• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) • Obsługa protokołu Diffiego-Hellman grup 19 i 20 • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth • Mechanizm „Split tunneling” dla połączeń Client-to-Site 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej. 4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)	
8	Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego • Policy Based Routingu • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.	

9	Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	
10	Kontrola Antywirusowa	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2121). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanymi dotąd zagrożeń	
11	Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.	
12	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2800 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	

13	Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	
14	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
15	Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	

		4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	
16	Serwisy i licencje	Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy	
17	Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.	

Podpis elektroniczny –szt.

Certyfikat kwalifikowany musi być ważny przez co najmniej 3 lata. Każdy certyfikat powinien zawierać min 1350 znaczników czasu/miesiąc.

Zamawiający nie dopuszcza w ramach realizacji przedmiotu umowy dokonywania przedpłat za wydawane certyfikaty oraz zawierania umów indywidualnych z każdym posiadaczem elektronicznego certyfikatu. Zamawiający wymaga dostarczenia działającego certyfikatu w ciągu 5 dni roboczych od momentu dostarczenia kompletnego zamówienia niezbędnego do jego wygenerowania (bez dodatkowych operacji związanych z oczekiwaniem na kody aktywacyjne, autoryzujące itp).

Oferta powinna zawierać wszystkie koszty związane z obsługą formalnoprawną i logistyczną procesu wydawania i unieważnienia certyfikatów

LP	Parametr lub warunek	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
1	Certyfikat:	1) Certyfikat kwalifikowany i certyfikat niekwalifikowany muszą być przechowywane w pamięci karty kryptograficznej 2) Dostawca usług certyfikacyjnych musi być kwalifikowanym podmiotem świadczącym usługi certyfikacyjne wpisanym do stosownego rejestru określonego w Rozporządzeniu Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym i towarzyszącym im rozporządzeniom wykonawczym.	
2	Czytnik kart kryptograficznych	1) Zgodność ze standardem PC/SC. 2) Obsługa kart procesorowych zgodnych z normami ISO 7816-1, ISO 7816-2, ISO 7816-3, ISO 7816-4. 3) Obsługa kart identyfikacyjnych formatu ID-1 zgodnych z normą ISO/IEC 7810. 4) Obsługa protokołów T=0 i T=1. 5) Obsługa w systemach operacyjnych: MS Windows 7/8/10, opcjonalnie Linux. 6)	

3	Karta kryptograficzna	1) Karta kryptograficzna wraz z programowaniem do składania bezpiecznego podpisu elektronicznego musi być zgodna z wymogami Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. 2) Karta kryptograficzna musi być zgodna z normami ISO 7816-1, ISO 7816-2, ISO 7816-3, ISO 7816-4. 3) Karta kryptograficzna musi posiadać pamięć nie mniejszą niż 64 kilobajty 4) Karta kryptograficzna musi umożliwiać przechowywanie w swojej pamięci jednej pary kluczy prywatnych do składania bezpiecznego podpisu elektronicznego zgodnego z ustawą o podpisie elektronicznym wraz z certyfikatem kwalifikowanym oraz minimum dwóch par kluczy kryptograficznych dla certyfikatów niekwalifikowanych wraz z certyfikatami, chronionych oddzielnymi kodami PIN dla każdej pary kluczy. 5) Karta kryptograficzna musi zapewniać wsparcie dla standardów przemysłowych (PKCS#11, #15, MS CAPI, PC/SC). 6) Karta kryptograficzna musi umożliwiać przechowywanie i wykorzystanie kluczy kryptograficznych RSA o długości co najmniej 2048 bitów 7) Wykonawca dostarcza kartę kryptograficzną wraz z oprogramowaniem zarządzającym certyfikatami kwalifikowanym i niekwalifikowanym zapisanymi na karcie kryptograficznej. Dostarczone oprogramowanie musi zapewnić obsługę kart kryptograficznych w systemach operacyjnych MS Windows 7/8/10, opcjonalnie Linux	
4	Oprogramowanie	Wykonawca dostarcza oprogramowanie które musi umożliwiać składanie bezpiecznego podpisu elektronicznego zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Aplikacja musi umożliwiać: - masowe i szybkie składanie oraz weryfikacja podpisów, poprzez: - wskazywanie wielu plików do strumieniowego podpisania lub weryfikacji, - określenie limitu czasu lub limitu ilości operacji kryptograficznych, do osiągnięcia których możliwe będzie wykorzystywanie komponentu technicznego po jednokrotnym podaniu kodu PIN; - składanie podpisu elektronicznego w jednym z formatów dopuszczonych przez rozporządzenie eIDAS: * CAdES (PKCS#7) - aplikacja obsługuje warianty: CAdES-BES, CAdES-T, oraz umożliwia składanie podpisu wielokrotnego. * XAdES - aplikacja obsługuje warianty: XAdES-BES, XAdES-T, XAdES-C, XAdES-A oraz umożliwia składanie podpisu wielokrotnego, kontrasygnaty, czy podpisu otaczanego.	

	* PAdES - aplikacja obsługuje warianty: PAdES-BES, PAdES-T, PAdES-LTV. * ASiC-S - aplikacja obsługuje warianty: ASiC-S-CAdES-BES, ASiC-S-XAdES-BES, ASiC-S-CAdES-T, ASiC-S-XAdES-T. * możliwość szyfrowania i deszyfrowania plików przy pomocy certyfikatów niekwalifikowanych algorytmami DES3 i AES; * możliwość przygotowania szablonów podpisywania i weryfikowania dokumentów; * obsługa kart kryptograficznych wydawanych przez wszystkie kwalifikowane centra certyfikacji działające na polskim rynku;	
--	---	--

Centrala Telefoniczna – 2 szt

Producent.....

Model

LP	Minimalne wymagania	Parametry oferowanego sprzętu, w szczególności potwierdzające spełnienie wymagań Zamawiającego
konfiguracja	- 4 x LM analogowa, - 32 numery wewnętrzne analogowe, - z modułem 1 bramy GSM - ze sterownikiem LAN/8VoIP/12Rec (aktywne 4 kanały REC)* - z licencją na program RECORDMAN2 Serwer - z kartą pamięci podręcznej SD 16GB - w obudowie RACK - rejestracja rozmów	
Wyposażenie	współpraca ze stykami S0 ISDN-BRA, S2M ISDN-PRA (30B+D) i liniami POTS, wewnętrzne porty analogowe, cyfrowe systemowe i cyfrowe ISDN-BRA, prezentacja numeru CLIP na wewnętrznych liniach cyfrowych i analogowych, obsługa prezentacji numeru CLIP zewnętrznych portów cyfrowych i analogowych (FSK), praca w systemie impulsowym i tonowym, modem zdalnego zarządzania centralą, billing rozmów wychodzących (nr abonenta inicjującego rozmowę, ewentualny pośrednik, nr wybierany, data, godzina, koszt rozmowy), pełna rejestracja rozmów przychodzących (w tym również nieodebranych i złośliwych) z informacją, który abonent odebrał rozmowę, pełna obsługa połączeń przychodzących w konfiguracji MSN i DDI, zapewniająca bezpośrednie wybieranie z "miasta" nr wewnętrznych, funkcja LCR-wyбір najtańszej drogi połączeniowej, System DISA umożliwiający dostęp do nr wewnętrznych, 99 zapowiedzi słownych (pierwszych 10 po 120 s, pozostałe po 30 s) abonenci wirtualni (konta),	

	współpraca z cyfrowymi telefonami systemowymi, współpraca z bramofonami, współpraca z bramką GSM, współpraca z systemem DECT, współpraca z systemami VoIP, współpraca z siecią komputerową w ramach systemu wspomagania telefonów CTI	
--	--	--

Serwer usług WEB:

W ramach wdrożenia należy zapewnić usługę hostingową serwera na okres 36 miesięcy w jednym z centrów hostingowych.

Wymagania odnośnie serwerowni dostawcy usługi:

- możliwość kolokacji pojedynczych urządzeń w obudowie rack oraz w obudowie wolnostojącej, a także szaf teletechnicznych 48U
- możliwość dzierżawy i kolokacji fizycznych serwerów dedykowanych
- kontrolę dostępu do pomieszczeń kolokacyjnych oraz monitoring wideo i fizyczną ochronę budynku
- system przeciwpożarowy z systemem gaszenia gazem
- trzy poziomy systemy gwarantowanego zasilania
- min 3 niezależne połączenia światłowodowe do naszych węzłów zlokalizowanych w punktach wymiany ruchu.

Standardowe SLA [roczne] dla infrastruktury sieciowej oraz zasilania DataHouse :

- dostęp do sieci Internet – 99,98%,
- zasilanie – 99,999%

Usługa o parametrach nie gorszych niż:

- a) Procesor klasy Intel Core i5-3570 – lub równoważny
- b) Pamięć RAM – min 16 GB
- c) Przestrzeń HDD min 2 dyski o pojemności min 500 GB każdy
- d) Min 1 interfejs sieciowy Ethernet
- e) adresacja IPv4 – 4 adresy [1 adres użytkowy]
- f) dedykowane łącze symetryczne o przepustowości min 25 Mb/s bez limitów transferu. CIR 100%
- g) usługa zdalnego restartu
- h) min 1 port ETH 1 Gb/s na switchu dostępowym

Powiadomienia SMS – 25 000 szt.

W ramach wdrożenia należy zapewnić możliwość wysłania 25 000 powiadomień SMS do pacjentów. Dzięki usłudze, placówka medyczna dysponuje możliwością realizowania wysyłki SMS wg zaplanowanego harmonogramu, oraz udzielanie odpowiedzi przez pacjenta np. w celu potwierdzenia czy odrzucenia terminu wizyty. Dzięki przypomnieniom zmniejszy liczbę niezrealizowanych wizyt, zaoszczędzisz czas i pieniądze.

OŚWIADCZAM (MY) , ŻE OFEROWANY PRZEDMIOT ZAMÓWIENIA SPEŁNIA WSZYSTKIE W/W WYMAGANIA:

Załącznik stanowi integralną część oferty.

Miejscowość, data:

.....
pieczęć i podpis osób uprawnionych
lub czytelny podpis osób uprawnionych