PARAMETRY WYMAGANE

1. **Szczegółowa specyfikacja techniczna proponowanego przełącznika głównego sieci LAN – 1 Kpl. - parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

Opis parametru	Wymagane minimalne parametry	Oferowane (spełnia/ nie spełnia)
Minimalne wymagania sprzętowe		
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Obudowa modularna przeznaczona do montażu w szafie 19”. Wysokość obudowy nie większa niż 10 RU	TAK	
2 karty zarządzające	TAK	
Minimum 12 portów 10G Ethernet ze stykiem SFP+ z możliwością zainstalowania modułów 10G w tym: SR, LR, ER	TAK	
Urządzenie musi być wyposażone we wkładki SFP+ odpowiednie do typu światłowodu - multimode oraz odpowiedniej ilości koniecznej do uruchomienia szkieletu sieci LAN - min. 12 szt.	TAK	
Minimum 48 portów Gigabit Ethernet 10/100/1000 RJ45 (Auto-MDIX) z obsługą standardów 802.3af i 802.3at działających bez nadsubskrypcji względem matrycy przełączającej	TAK	
Urządzenie powinno posiadać minimum 2 niezależne zasilacze 230V AC posiadające po minimum 1440W dostępnej mocy dla funkcjonalności PoE i PoE+	TAK	
Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie oraz aby karty z tymi portami posiadały przełączanie lokalne (rozproszona architektura przełączania)	TAK	
Wymagane jest zapewnienie min. czterech dodatkowych wolnych slotów na karty liniowe celem przyszłej rozbudowy	TAK	
Wolne sloty na karty liniowe muszą umożliwić rozbudowę o co najmniej 160 portów 10 Gigabit Ethernet lub 192 portów Gigabit Ethernet	TAK	
Przepustowość od karty liniowej do matryc przełączających	Minimum 60 Gb/s full-duplex per slot	
Wydajność pojedynczej matrycy przełączającej	Minimum 512 Gb/s	
Możliwość wymiany zasilaczy i wentylatorów w trakcie pracy urządzenia bez wpływu na jego działanie	TAK	
Możliwość łączenia dwóch przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree	TAK	
Przełączanie w warstwie drugiej i trzeciej modeli ISO/OSI	TAK	
Port konsoli - szeregowy RS-232	TAK	
Możliwość instalacji kart liniowych posiadających zarówno porty 100/1000M SFP jak i 10/100/1000M RJ45 na jednej karcie	TAK	

Możliwość instalacji kart liniowych posiadającej zarówno porty 100/1000M SFP jak i 10G XFP lub SFP+ na jednej karcie	TAK	
Port do zarządzania poza pasmem	10/100M RJ45	
Funkcje warstwy 2		
GARP VLAN Registration Protocol (GVRP)	TAK	
Rozmiar tablicy MAC min. 32 000 adresów	TAK	
4094 sieci VLAN	TAK	
IEEE 802.1ad QinQ i Selective QinQ	TAK	
Agregacja portów statyczna i przy pomocy protokołu LACP	TAK	
Min. 20 grup portów zagregowanych, możliwość stworzenia grupy z min. 8 portów	TAK	
Spanning Tree: MSTP 802.1s, RSTP 802.1w, STP Root Guard	TAK	
64 instancje MSTP 802.1s	TAK	
Funkcje warstwy 3		
routing IPv4 z prędkością łącza	TAK	
wsparcie dla routingu IPv4: statycznego , RIP i RIPv2, OSPF, IS-IS i BGP	TAK	
routing IPv6 z prędkością łącza	TAK	
wsparcie dla routingu IPv6: statycznego, RIPng, OSPFv3, IS-ISv6 i BGP4+	TAK	
Jeżeli funkcjonalność routingu IPv6 wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach niniejszego postępowania	TAK	
Rozmiar tablic przełączania FIB dla IPv4 na kartach zarządzających i na każdej karcie liniowej oddzielnie: min. 12 000 wpisów	TAK	
Rozmiar tablic przełączania FIB dla IPv6 na kartach zarządzających i na każdej karcie liniowej oddzielnie: min. 6 000 wpisów	TAK	
Bidirectional Forwarding Detection dla OSPF, BGP, IS-IS, VRRP	TAK	
Virtual Router Redundancy Protocol (VRRP)	TAK	
Policy-based routing	TAK	
IGMPv1, v2, and v3	TAK	
PIM-SSM, PIM-DM i PIM-SM	TAK	
NSF	TAK	
Bezpieczeństwo		
Zaawansowany mechanizm kolejkowania procesora zapobiegający atakom DoS	TAK	
Minimum 2 000 list kontroli dostępu (ACL)	TAK	
DHCP snooping	TAK	
RADIUS	TAK	
Secure Shell (SSHv2)	TAK	
IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs: zezwalające na nadzór nad dostępem użytkownika do sieci	TAK	
Guest VLAN	TAK	
Port isolation	TAK	
Port security: zezwalający na dostęp tylko specyficznym adresom MAC	TAK	
MAC-based authentication	TAK	
IP source guard	TAK	
URPF	TAK	

Quality of Service (QoS)		
Funkcje QoS: kreowanie klas ruchu w oparciu o access control lists (ACLs), IEEE 802.1p precedence, IP, DSCP oraz Type of Service (ToS) precedence	TAK	
Wsparcie dla następujących metod zapobiegania zatorom: priority queuing, weighted round robin (WRR), weighted random early discard (WRED), deficit round robin (DRR)	TAK	
Min. 8 kolejek wyjściowych na każdy port 10G i 1G Ethernet kart liniowych przełącznika, z możliwością ich konfigurowania przez użytkownika (m.in. definiowanie algorytmu kolejkowania, przypisania poszczególnych klas ruchu do danej kolejki).	TAK	
Urządzenie musi posiada mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający nie wymaga jej dostarczenia w ramach niniejszego postępowania	TAK	
Monitoring i diagnostyka		
Port mirroring	TAK	
OAM (802.3ah) i CFD (802.1ag): wykrywanie problemów na łączu pomiędzy urządzeniami	TAK	
Zarządzanie		
Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI)	TAK	
IEEE 802.1ab LLDP	TAK	
Usługi DHCP: serwer (RFC 2131), klient i relay	TAK	
SNMPv1, v2c, and v3	TAK	
Syslog	TAK	
Gwarancja i serwis		
Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy	TAK	
Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski	TAK	
Zamawiający wymaga, aby dostarczony przełącznik sieciowy posiadał gwarancję minimum 3 lata, świadczoną przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu	TAK	

zdawczo-odbiorczego przedmiotu zamówienia		
Bezpłatna aktualizacja oprogramowania urządzenia przez cały okres gwarancji urządzenia	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

2. Szczegółowa specyfikacja techniczna proponowanego przełącznika dostępowego sieci LAN (typ I) – 12 Kpl. – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Parametry fizyczne	Wysokość max 1 RU Montaż w szafie 19” Głębokość nie większa niż 46cm	
Zasilanie	1 wewnętrzny zasilacz 230V AC	
Zasilanie nadmiarowe	Możliwość zastosowania zasilacza nadmiarowego (dopuszczalne rozwiązania zewnętrzne)	
Zakres temperatur pracy	0 – 45 °C	
Ilość portów 10/100/1000M RJ45	Minimum 24 porty Gigabit Ethernet 10/100/1000 RJ45 (Auto-MDIX) z obsługą standardów 802.3af i 802.3at (min. 370W dostępnej mocy PoE)	
Ilość portów 10G SFP+	Minimum 2 porty 10G SFP+	
Urządzenie musi być wyposażone we wkładki SFP+ odpowiednie do typu światłowodu - multimode oraz odpowiedniej ilości koniecznej do uruchomienia szkieletu sieci LAN	TAK	
Wszystkie porty 10Gb/s muszą umożliwiać pracę z wkładkami SFP+: 10GBase-SR, 10GBase-LRM, 10GBase-LR oraz z wkładkami SFP: 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-BX, CWDM	TAK	
Przełącznik musi umożliwiać jednoczesne wykorzystanie minimum 26 portów	TAK	
Przełącznik musi umożliwiać łączenie w stos składający się z minimum 9 urządzeń	TAK	
Zarządzanie stosem poprzez jeden adres IP	TAK	
Magistrala stackująca w topologii pierścienia o wydajności co najmniej 40Gb/s	TAK	
Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)	TAK	
Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu	TAK	

Spanning-Tree		
Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych modułów stackujących lub licencji to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. W ramach niniejszego postępowania Zamawiający nie wymaga dostarczenia kabli stakujących	TAK	
Zamawiający dopuszcza możliwość aby funkcja łączenia w stos odbywała się za pomocą portów 10G SFP+. W takim wypadku urządzenie musi umożliwiać jednoczesne wykorzystanie 24 portów 10/100/1000 RJ45, 2 portów 10G SFP+ oraz dodatkowych portów 10G SFP+ do realizacji funkcji stackowania.	TAK	
Matryca przełączająca o wydajności min. 176Gbps, wydajność przełączania przynajmniej 65 mpps	TAK	
Pojemność tablicy MAC	16 000	
Ilość obsługiwanych jednocześnie sieci VLAN	1 000	
Obsługa 802.1Q tunneling (QinQ)	TAK	
Minimalna wielkość obsługiwanych ramek jumbo	9216 B	
Spanning Tree	MSTP 802.1s, RSTP 802.1w, STP Root Guard	
Ilość instancji MSTP 802.1s	64	
Ilość obsługiwanych statycznych tras dla routingu IPv4	Minimum 16	
Ilość obsługiwanych statycznych tras dla routingu IPv6	Minimum 16	
Obsługa protokołów LLDP i LLDP-MED	TAK	
Przełącznik musi posiadać funkcjonalność DHCP Snooping	TAK	
Obsługa ruchu multicast – IGMP Snooping v3 i MLD Snooping	TAK	
Ilość poziomów dostępu administracyjnego poprzez konsolę	Minimum 4	
Ilość jednocześnie obsługiwanych list kontroli dostępu (ACL)	Minimum 400	
Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL	TAK	
Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC	TAK	
Zarządzanie urządzeniem	HTTPS, SNMPv2, SNMPv3 i SSHv2	
Możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP	TAK	
Obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny)	TAK	
Możliwość synchronizacji czasu zgodnie z NTP	TAK	
Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym	TAK	
Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów	źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP	
Obsługa jednej z powyżej wspomnianych kolejek z	TAK	

bezwzględnym priorytetem w stosunku do innych (Strict Priority)		
Możliwość ograniczania ruchu przychodzącego i wychodzącego na portach w przedziale od 64kb/s do przepustowości maks. portu z granulacją 8 kb/s	TAK	
Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania	TAK	
Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN	TAK	
Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)	TAK	
Wbudowana pamięć flash dostępna na urządzeniu	Minimum 64 MB	
Dedykowany port konsoli USB	TAK	
Przełącznik musi być zgodny z normami środowiskowymi, bezpieczeństwa oraz kompatybilności elektromagnetycznej	EN 60950-1 EN 55022 klasa A EN300386 EN61000-4-2 EN61000-4-4 EN61000-4-5 EN61000-4-6 Reduction of Hazardous Substances (RoHS)	
Wszystkie dostarczone wkładki SFP+ muszą pochodzić od tego samego producenta co oferowane przełączniki, muszą być z nimi kompatybilne i objęte takim samym serwisem gwarancyjnym jak przełączniki	TAK	
Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy	TAK	
Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia	TAK	

przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski		
Zamawiający wymaga, aby wszystkie dostarczone przełączniki sieciowe posiadały gwarancję minimum 3 lata, świadczoną przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia	TAK	
Bezpłatna aktualizacja oprogramowania urządzenia przez cały okres gwarancji urządzeń	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

3. **Szczegółowa specyfikacja techniczna proponowanego przełącznika dostępowego sieci LAN (typ II) – 16 Kpl. – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Parametry fizyczne	Wysokość max 1 RU Montaż w szafie 19” Głębokość nie większa niż 46cm	
Zasilanie	1 wewnętrzny zasilacz 230V AC	
Zasilanie nadmiarowe	Możliwość zastosowania zasilacza nadmiarowego (dopuszczalne rozwiązania zewnętrzne)	
Zakres temperatur pracy	0 – 45 °C	
Ilość portów 10/100/1000M RJ45	Minimum 48 portów Gigabit Ethernet 10/100/1000 RJ45 (Auto-MDIX) z obsługą standardów 802.3af i 802.3at (min. 370W dostępnej mocy PoE)	
Ilość portów 10G SFP+	Minimum 2 porty 10G SFP+	
Urządzenie musi być wyposażone we wkładki SFP+ odpowiednie do typu światłowodu - multimode oraz odpowiedniej ilości koniecznej do uruchomienia szkieletu sieci LAN	TAK	
Wszystkie porty 10Gb/s muszą umożliwiać pracę z wkładkami SFP+: 10GBase-SR, 10GBase-LRM, 10GBase-LR oraz z wkładkami SFP: 1000Base-SX, 1000Base-LX, 1000Base-ZX, 1000Base-BX, CWDM	TAK	
Przełącznik musi umożliwiać jednoczesne wykorzystanie minimum 50 portów	TAK	
Każde urządzenie musi zostać dostarczone z 2 wkładkami SFP+ 10GBase-SR	TAK	
Przełącznik musi umożliwiać łączenie w stos składający się z minimum 9 urządzeń	TAK	
Zarządzanie stosem poprzez jeden adres IP	TAK	
Magistrala stackująca w topologii pierścienia o wydajności co najmniej 40Gb/s	TAK	
Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)	TAK	
Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu	TAK	

Spanning-Tree		
Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych modułów stackujących lub licencji to w ramach niniejszego postępowania Zamawiający nie wymaga ich dostarczenia.	TAK	
Zamawiający dopuszcza możliwość aby funkcja łączenia w stos odbywała się za pomocą portów 10G SFP+. W takim wypadku urządzenie musi umożliwiać jednoczesne wykorzystanie 48 portów 10/100/1000 RJ45, 2 portów 10G SFP+ oraz dodatkowych portów 10G SFP+ do realizacji funkcji stackowania.	TAK	
Matryca przełączająca o wydajności min. 176Gbps, wydajność przełączania przynajmniej 101 mpps	TAK	
Pojemność tablicy MAC	16 000	
Ilość obsługiwanych jednocześnie sieci VLAN	1 000	
Obsługa 802.1Q tunneling (QinQ)	TAK	
Minimalna wielkość obsługiwanych ramek jumbo	9216 B	
Spanning Tree	MSTP 802.1s, RSTP 802.1w, STP Root Guard	
Ilość instancji MSTP 802.1s	64	
Ilość obsługiwanych statycznych tras dla routingu IPv4	Minimum 16	
Ilość obsługiwanych statycznych tras dla routingu IPv6	Minimum 16	
Obsługa protokołów LLDP i LLDP-MED.	TAK	
Przełącznik musi posiadać funkcjonalność DHCP Snooping	TAK	
Obsługa ruchu multicast – IGMP Snooping v3 i MLD Snooping	TAK	
Ilość poziomów dostępu administracyjnego poprzez konsolę	Minimum 4	
Ilość jednocześnie obsługiwanych list kontroli dostępu (ACL)	Minimum 400	
Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL	TAK	
Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC	TAK	
Zarządzanie urządzeniem	HTTPS, SNMPv2, SNMPv3 i SSHv2	
Możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP	TAK	
Obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny)	TAK	
Możliwość synchronizacji czasu zgodnie z NTP	TAK	
Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym	TAK	
Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów	źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP	
Obsługa jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)	TAK	

Możliwość ograniczania ruchu przychodzącego i wychodzącego na portach w przedziale od 64kb/s do przepustowości maks. portu z granulacją 8 kb/s	TAK	
Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania	TAK	
Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN	TAK	
Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)	TAK	
Wbudowana pamięć flash dostępna na urządzeniu	Minimum 64 MB	
Dedykowany port konsoli USB	TAK	
Przełącznik musi być zgodny z normami środowiskowymi, bezpieczeństwa oraz kompatybilności elektromagnetycznej	EN 60950-1 EN 55022 klasa A EN300386 EN61000-4-2 EN61000-4-4 EN61000-4-5 EN61000-4-6 Reduction of Hazardous Substances (RoHS)	
Wszystkie dostarczone wkładk i SFP+ muszą pochodzić od tego samego producenta co oferowane przełączniki, muszą być z nimi kompatybilne i objęte takim samym serwisem gwarancyjnym jak przełączniki	TAK	
Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy	TAK	
Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski	TAK	
Zamawiający wymaga, aby wszystkie dostarczone	TAK	

przełączniki sieciowe posiadały gwarancję minimum 3 lata, świadczoną przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia		
Bezpłatna aktualizacja oprogramowania urządzenia przez cały okres gwarancji urządzeń	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

4. Szczegółowa specyfikacja techniczna proponowanej systemu zapór ogniowych – 2 Kpl. – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Przepustowość urządzenia minimum 20 Gbps	TAK	
Przepustowość dla pakietów o różnej wielkości minimum 10 Gbps	TAK	
Liczba nowych połączeń na sekundę minimum 300 000	TAK	
Liczba jednoczesnych połączeń minimum 8 000 000	TAK	
Możliwość rozszerzenia funkcjonalności o SSL VPN za pomocą dodatkowej licencji z minimalną obsługą 200 jednoczesnych połączeń.	TAK	
Liczba jednoczesnych połączeń IPSec VPN minimum 10 000	TAK	
Przepustowość IPsec VPN min. 5 Gbit/s	TAK	
Dedykowany system operacyjny opracowany przez producenta urządzenia	TAK	
Minimum 8 portów GigabitEthernet 10/100/1000 z możliwością rozbudowy do 4 portów 10 Gigabit Ethernet i 12 portów GigabitEthernet 10/100/1000	TAK	
Urządzenie musi posiadać minimum 2 dodatkowe sloty na porty, w tym moduły z portami 10 Gigabit Ethernet	TAK	
Inteligentna kontrola temperatury oraz automatyczne dostosowanie prędkości wiatraków	TAK	
Urządzenie wyposażone w 2 zasilacze AC pracujące w konfiguracji 1+1 przy czym jeden moduł zasilacza musi wystarcz do zasilenia urządzenia	TAK	
Urządzenie o wysokości do-3U	TAK	
Urządzenie musi posiadać minimum 16GB wbudowanej pamięci RAM	TAK	
Urządzenie musi posiadać minimum 8GB pamięci flash	TAK	
Możliwość uruchomienia firewalla w trybie routingu lub transparentnym	TAK	
Mechanizmy ochrony sieci IP w wersji 4	TAK	
Mechanizmy ochrony sieci IP w wersji 6	TAK	
Obsługa protokołów rutingu RIP, OSPF, BGP, IS-IS, obsługa	TAK	

rutingu multicast'owego (MSDP, PM-DM, PM-SM, IGMP oraz statycznego rutingu multicast'owego).		
Możliwość konfiguracji przez użytkownika tzw. Policy Based Routing (PBR).	TAK	
Wspierane protokoły oraz funkcjonalności dla IPv6: Adresacja interfejsów dla IPv6, NDP, NAT64 oraz DHCP relay	TAK	
Mechanizmy migracji do IPv6: dual-stack	TAK	
Routing dla IPv6: OSPFv3, routing statyczny	TAK	
Wymagana funkcjonalności IPS. Urządzenie dostarczone wraz z licencjami do aktualizacji przez okres 3 lat.	TAK	
Możliwość uruchomienia przynajmniej do 8 interfejsów fizycznych jako jedno łącze logiczne w celu zwiększenia przepustowości i niezawodności połączenia.	TAK	
Logowanie w formie sysloga.	TAK	
Możliwość rozszerzenia o funkcjonalność wirtualnych firewalli za pomocą dodatkowej licencji z obsługą minimum 100 wirtualnych urządzeń.	TAK	
Możliwość uruchomienia funkcjonalności NAT w tym translacja adresu IP źródłowego, translacja adresu IP przeznaczenia, PAT, translacja statyczna i translacje puli adresów IP.	TAK	
Inspekcja różnych protokołów w celu przepuszczenia odpowiedniego ruchu w tym FTP, H323, RAS, SIP, ICMP, RTSP, NetBios, ILS, PPTP, SQL.NET.	TAK	
Możliwość konfiguracji kontroli dostępu na podstawie adresów źródłowych i przeznaczenia, portów, typu protokołu, czasu, TOS.	TAK	
Wsparcie dla inspekcji aplikacji opartych o protokoły TCP/UDP oraz takie protokoły jak FTP, SMTP, HTTP, RTSP, H323, SIP, blokowanie Java applet/ActiveX.	TAK	
Ochrona przed atakami typu SYN flood.	TAK	
Możliwość uruchomienia firewalla w trybie redundantnej pracy dla zwiększenie niezawodności.	TAK	
Praca w trybie redundancji active-active oraz active-standby	TAK	
Mechanizm redundancji systemu działa w trybie rutingu jak i transparentnym.	TAK	
Obsługa protokołów rutingu RIP, OSPF, OSPFv3, obsługa rutingu multicast'owego (PM-SM, IGMP).	TAK	
Możliwość konfiguracji przez użytkownika tzw. Policy Based Routing (PBR).	TAK	
Wsparcie dla protokołów tunelowania SSL VPN, IPSec VPN, L2TP VPN, L2TP over IPSec VPN.	TAK	
Wsparcie dla mechanizmów redundancji dla połączeń IPSec VPN.	TAK	
Tryby pracy In-line oraz Off-line	TAK	
Wykrywanie anomalii w różnych protokołach: HTTP, SMTP, FTP, POP3, IMAP4, NETBIOS, SMB, MS_SQL, Telnet, IRC oraz DNS	TAK	

Grupowanie baz sygnatur na kategorie	TAK	
Wspieranie baz sygnatury definiowanych przez użytkownika	TAK	
Automatyczna aktualizacja bazy sygnatur poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji	TAK	
Możliwość powiązania polityk bezpieczeństwa IPS z regułami ACL	TAK	
Możliwość włączania i wyłączania jednej lub wszystkich reguł w polityce bezpieczeństwa oraz konfiguracji rodzaju reakcji na zdarzenie	TAK	
Możliwość włączenia i wyłączenia funkcji IPS globalnie dla całego urządzenia	TAK	
Możliwe rodzaje reakcji na zdarzenie: logowanie i blokowanie pakietów	TAK	
Wysyłanie logów do zewnętrznego serwera oraz generowanie różnych rodzajów raportów umożliwiających sprawdzenie najczęściej występujących ataków, ich adresów źródłowych i przeznaczenia	TAK	
Reakcja w przypadku awarii modułu (w zależności od ustawień): przesłanie danych dalej lub blokada	TAK	
Możliwość zarządzanie w sposób graficzny przy wykorzystaniu protokołów HTTP i HTTPS	TAK	
Możliwość konfiguracji z poziomu linii komend poprzez TELNET i SSH. Dostęp do pomocy w języku angielskim	TAK	
Funkcjonalność debugowania pakietów przez port szeregowy w celu analizy i rozwiązywania problemów	TAK	
Tworzenie kopii zapasowych konfiguracji, eksportowanie i przywracanie.	TAK	
Urządzenie musi posiadać możliwość rozszerzenia za pomocą dodatkowej licencji o funkcjonalność anti-virus, z parametrami pracy opisanymi poniżej	TAK	
Skanowanie różnych protokołów w celu wykrycia wirusów w plikach przesyłanych przez HTTP, SMTP, POP3 oraz FTP	TAK	
Dekompresja wielokrotnie skompresowanych plików.	TAK	
Możliwość automatycznej aktualizacji bazy wirusów poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji.	TAK	
Możliwość wylistowania wirusów zawartych w bazie.	TAK	
Możliwość usunięcia wirusa, wyświetlenia strony alarmującej, oznaczanie wiadomości mailowej oraz logowanie.	TAK	
Konfiguracja polityki - możliwość powiązania polityk AC z regułami ACL.	TAK	
Możliwość włączenia i wyłączenia funkcji AV globalnie dla całego urządzenia.	TAK	
Możliwość wysyłania logów do serwera syslog oraz obsługa raportów różnego typu.	TAK	
Reakcja w przypadku awarii modułu - w zależności od ustawień przesłanie danych dalej lub blokada w przypadku przeciążenia modułu AV	TAK	

Urządzenie musi posiadać możliwość rozszerzenia za pomocą dodatkowej licencji o funkcjonalność filtrowania adresów URL, z parametrami pracy opisanymi poniżej	TAK	
Dostęp do strony zainicjowany z adresu IP znajdującego się w liście wprowadzonych adresów nie jest filtrowany i ma najwyższy priorytet.	TAK	
Obsługa dopasowywania wpisów w tzw. whitelist oraz blacklist w oparciu o prefiks, sufiks słowa kluczowego. Blacklist i whitelist mają wyższy priorytet niż kategoria URL. Whitelist ma wyższy priorytet niż blacklist	TAK	
Obsługa kategorii URL tworzonych przez użytkownika. Kategorie stworzone przez użytkownika mają wyższy priorytet od predefiniowanych kategorii	TAK	
Możliwość dodania adresu URL do danej kategorii lub zapytania o kategorie danego adresu URL	TAK	
Filtrowanie oparte o kategorie uzyskiwane z serwera kategorii URL	TAK	
Możliwość otrzymywania kategorii z serwera kategorii dostępnego w sieci Internet. Reakcja podejmowana jest na podstawie skonfigurowanej polityki i przypisanej akcji do konkretnej grupy URL	TAK	
Konfiguracja polityki filtracji adresów URL	TAK	
Możliwość wyświetlenia częściowo kastomizowanej strony informującej o zablokowaniu dostępu	TAK	
Polityka filtrowania URL może być oparta o grupę adresów i określony czas.	TAK	
Możliwość filtrowania stron z określeniem słów kluczowych występujących w treści strony.	TAK	
Możliwość blokowania prób wyszukania konkretnych słów kluczowych przez wyszukiwarki internetowe.	TAK	
Możliwość filtrowania publikacji konkretnych słów kluczowych	TAK	
Kontrola postów na portalach internetowych	TAK	
Kontrola ściągania i wysyłania plików poprzez określenie nazwy plików, rodzaju lub rozmiaru	TAK	
Funkcja logowania dostępu do adresów URL. Możliwość określenia osiągniętych zasobów.	TAK	
Możliwość scalania logów	TAK	
Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy	TAK	
Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność	TAK	

uprawnień gwarancyjnych na terenie Polski		
Zamawiający wymaga, aby wszystkie dostarczone urządzenia posiadały gwarancję minimum 3 lata, świadczoną przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia	TAK	
Zamawiający wymaga aby wszystkie dostarczone firewalle posiadały licencję na funkcjonalność IPS wraz z możliwością aktualizacji przez okres 3 lat	TAK	
Bezpłatna aktualizacja oprogramowania urządzenia przez cały okres gwarancji urządzeń	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

4. Szczegółowa specyfikacja techniczna proponowanego urządzenia na styku z Internetem – 1 Kpl. - parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Urządzenie musi być routerem modularnym wyposażonym w minimum 7 interfejsów Gigabit Ethernet 10/100/1000BASE-T, z czego minimum 3 interfejsy muszą pracować jako porty typu WAN oraz jeden z interfejsów musi mieć możliwość pracy w trybie „dual-physical" z gigabitowym portem światłowodowym definiowanym przez wkładkę SFP	TAK	
Urządzenie musi być wyposażone w minimum 2GB pamięci Flash	TAK	
Urządzenie musi być wyposażone w minimum 2GB pamięci RAM	TAK	
Urządzenie musi być wyposażone w minimum trzy porty USB. Co najmniej dwa porty USB muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych. Co najmniej jeden port musi pełnić funkcję konsoli szeregowej	TAK	
Urządzenie musi być urządzeniem modularnym posiadającym możliwość instalacji co najmniej: 5 modułów sieciowych z interfejsami, oraz minimum 1 modułu z układami DSP	TAK	
Urządzenie musi posiadać zainstalowany sprzętowy moduł akceleracji szyfrowania DES/3DES/AES	TAK	
Urządzenie musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów	TAK	
Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł muszą mieć możliwość obsadzenia modułami: z przełącznikiem Ethernet o gęstości co najmniej 24 porty na moduł, z portami szeregowymi, z portami FXS, z portami FXO, z portami ISDN	TAK	
Slot urządzenia przewidziany pod rozbudowę o moduł z układem DSP musi mieć możliwość obsadzenia modułem o gęstości nie mniejszej niż 128 kanałów	TAK	
Urządzenie powinno charakteryzować się wydajnością minimum 1Mpps dla pakietów o wielkości 64B	TAK	
Oczekiwana wydajność proponowanego rozwiązania	TAK	

z włączonymi usługami nie może być mniejsza niż 350Mbit/s		
Oczekiwana wydajność proponowanego rozwiązania dla transmisji ruchu IPsec nie może być mniejsza niż 500Mbit/s	TAK	
Urządzenie musi obsługiwać jednocześnie 3 000 tuneli IPSec	TAK	
Urządzenie musi pozwalać na rozbudowę o funkcjonalność kontrolera WLAN za pomocą licencji lub dodatkowego modułu instalowanego w urządzeniu	TAK	
Oprogramowanie urządzenia musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji	TAK	
Urządzenie musi posiadać obsługę protokołów routingu IPv4: RIPv1, RIPv2, OSPF, ISIS, BGP oraz ruchu multicastowego: PIM-DM, PIM-SM, PIM-SSM	TAK	
Urządzenie musi posiadać obsługę protokołów routingu IPv6: RIPng, BGPv4, OSPFv3, IS-ISv6	TAK	
Urządzenie musi wspierać protokół BGP z obsługą 4 bajtowych ASN	TAK	
Urządzenie musi posiadać wsparcie dla funkcjonalności Policy Based Routing	TAK	
Urządzenie musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMPv3, IGMP Snooping, PIMv2	TAK	
Urządzenie musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)	TAK	
Urządzenie musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q	TAK	
Urządzenie musi obsługiwać IPv6 w tym ICMP dla IPv6	TAK	
Urządzenie musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP	TAK	
Urządzenie musi posiadać obsługę NAT i PAT dla ruchu IP unicast	TAK	
Urządzenie musi posiadać obsługę mechanizmu DiffServ	TAK	
Urządzenie musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu	TAK	
Urządzenie musi zapewniać obsługę mechanizmów kolejkowania ruchu: z obsługą kolejki absolutnego priorytetu, ze statyczną alokacją pasma dla typu ruchu, WFQ	TAK	
Urządzenie musi obsługiwać mechanizm WRED	TAK	
Urządzenie musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu	TAK	
Urządzenie musi obsługiwać protokół NTP	TAK	
Urządzenie musi obsługiwać protokół DHCP w trybie pracy jako serwer i trybie pracy jako klient	TAK	
Urządzenie musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika)	TAK	
Urządzenie musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS oraz TACACS+ lub odpowiednika	TAK	

Urządzenie musi posiadać funkcjonalność firewalla	TAK	
Urządzenie musi posiadać możliwość zestawiania tuneli VPN z wykorzystaniem protokołu IPsec, IKEv1 i IKEv2	TAK	
Urządzenie musi być zarządzalne za pomocą portu konsoli, usługi SSH, telnet,GUI oraz SNMPv3	TAK	
Urządzenie musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow lub odpowiednika	TAK	
Urządzenie musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI)	TAK	
Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania minimum 10 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian	TAK	
Obudowa urządzenia musi być wykonana z metalu	TAK	
Urządzenie musi mieć możliwość montażu w szafie 19”.	TAK	
Wielkość urządzenie nie większa niż 3U	TAK	
Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem zmiennym 230V	TAK	
Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy	TAK	
Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski	TAK	
Zamawiający wymaga, aby dostarczone urządzenie posiadało gwarancję minimum 3 lata, świadczoną przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia	TAK	
Bezpłatna aktualizacja oprogramowania urządzenia przez cały okres gwarancji urządzenia	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

5. Szczegółowa specyfikacja techniczna proponowanego systemu bezpieczeństwa dostępu do sieci LAN – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Oferowany system musi pochodzi od tego samego producenta co oferowane urządzenia typu przełącznik główny, przełączniki dostępowe, system zapór ogniowych oraz urządzenie na styku z Internetem w celu zapewnienia jak najlepszej integracji i wykorzystaniu jak największej ilości funkcjonalności oferowanych przez taki system	TAK	
Pełna kompatybilność wymaganych funkcjonalności z oferowanymi urządzeniami typu przełącznik główny, przełączniki dostępowe, system zapór ogniowych oraz urządzenie na styku z Internetem	TAK	
Możliwość przypisywania różnych polityk bezpieczeństwa użytkownikom sieci Ethernet wraz z możliwością rozszerzenia o możliwość przypisywania różnych polityk bezpieczeństwa użytkownikom sieci WLAN	TAK	
Możliwość rozwiązywania problemu „dostępu z poziomu dowolnego urządzenia" poprzez egzekwowanie strategii bezpiecznego dostępu do sieci LAN	TAK	
Wbudowana funkcjonalność serwera uwierzytelniania z obsługą protokołu Radius	TAK	
Egzekwowanie polityk bezpieczeństwa na styku dostępu do sieci LAN z wykorzystaniem protokołu 802.1x i EAP	TAK	
Możliwość definiowania profilów i cech charakterystycznych urządzeń nie obsługujących protokołu 802.1x, w celu zapewnienia dostępu do sieci LAN	TAK	
Realizacja polityki bezpieczeństwa w obrębie przedsiębiorstwa za pomocą egzekwowanych na poziomie sieci Ethernet reguł dostępu i szyfrowania, w tym minimum przydzielenie numeru VLAN, przydzielenie reguły ACL, przydzielenie dynamicznych reguły ACL	TAK	
Możliwość przypisywania różnych polityk bezpieczeństwa w zależności od pory dnia	TAK	
Urządzenie musi być wyposażone w licencję umożliwiającą dostęp do sieci dla co najmniej 500 użytkowników oraz licencję umożliwiającą utworzenie i dostęp do 500 kont gościnnych	TAK	
Dostarczone licencje na ilość obsługiwanych użytkowników i kont muszą być bezterminowe	TAK	
Możliwość tworzenia lokalnej bazy użytkowników oraz integracji z zewnętrznymi bazami jak np. LDAP oraz AD	TAK	
Odróżnianie urządzeń należących do przedsiębiorstwa od osobistych urządzeń użytkowników, w szczególności urządzeń mobilnych	TAK	

Możliwość przypisania dla tego samego konta użytkownika różnych polityk bezpieczeństwa w zależności od identyfikacji urządzenia jako urządzenie przedsiębiorstwa czy prywatne urządzeni użytkownika	TAK	
W przypadku, gdy oprogramowanie korzysta z systemu licencjonowania powinna być zapewniona możliwość sprawdzenia zainstalowanej licencji oraz zmiany licencji	TAK	
Monitorowanie wykorzystania licencji i informowanie użytkownika systemu o przekroczenia limitów zainstalowanej licencji (np. podłączonych użytkowników)	TAK	
Dostępna w systemie dokumentacja w języku polskim lub angielskim	TAK	
Możliwość obsługi dostępu gościnnego	TAK	
Możliwość tworzenia wydruków zawierających informacje o utworzonym koncie użytkownika gościnnego	TAK	
Możliwość tworzenia specjalnych kont użytkowników posiadających uprawnienia do zakładania i kasowania kont użytkowników gościnnych	TAK	
Możliwość personalizowania serwisu WEB dla dostępu gościnnego poprzez możliwości umieszczenie logo Zamawiającego oraz definicję parametrów potrzebnych do uwierzytelnienia	TAK	
Możliwość definicji sposobu tworzenia kont gościnnych, w tym minimum: - tworzenie kont gościnnych przez administratora systemu - tworzenie kont gościnnych przez uprawnionego użytkownika - tworzenie kont gościnnych przez samych użytkowników gościnnych	TAK	
Możliwość definicji sposobu aktywowanie utworzonych kont gościnnych, w tym: - możliwość aktywowania kont gościnnych przez administratora systemu - możliwość aktywowania kont gościnnych przez uprawnionego użytkownika zdefiniowanego przez administratora systemu - możliwość aktywowania kont gościnnych przez samych użytkowników gościnnych	TAK	
Możliwość tworzenia kont użytkowników gościnnych z uprawnieniami ograniczonymi czasowo	TAK	
Możliwość szybkiego tworzenia dużej ilości kont użytkowników gościnnych	TAK	
Centralne zarządzanie systemem bezpieczeństwa dostępu z poziomu jednego interfejsu GUI	TAK	
Obsługiwana lokalna baza administratorów systemu	TAK	
Wymagany interfejs użytkownika w języku polskim lub angielskim	TAK	
Możliwość tworzenia kont zarządzających systemem o różnych poziomach uprawnień	TAK	
System musi być dostarczony wraz z platformą serwerową tego samego producenta co oprogramowanie, o parametrach spełniających wymagania specyfikacji	TAK	

rekomendowanej przez producenta systemu dla min. 60 urządzeń sieciowych i jednocześnie spełniających następujące minimalne wymagania: - obudowa przeznaczona do montażu w szafie 19” - maksymalna wysokość 2RU - 8 GB RAM - 2 procesory sześciordzeniowe min. 2.5GHz - min. 2 dyski 300GB SAS hotswap - sprzętowy kontroler RAID 0,1,5,10 - 4 interfejsy sieciowe GigabitEthernet - 5 slotów PCIe - 2 redundantne zasilacze - minimum 2 porty USB - niezależny od CPU kontroler zdalnego zarządzania serwerem z funkcją zdalnego restartu oraz zdalnej konsoli wspierającej systemy operacyjne z rodziny Linux, Windows. Jeżeli dla funkcjonalności zdalnego zarządzania wymagana jest licencja, zostanie ona dostarczona przez Wykonawcę		
System bezpieczeństwa dostępu do sieci LAN należy dostarczyć wraz z serwisem gwarancyjnym na minimum 3 lata	TAK	
Serwis ten musi zapewniać dostęp do zdalnego wsparcia technicznego producenta przez całą dobę, 7 dni w tygodniu	TAK	
Serwis musi zapewniać bezpłatny dostęp do poprawek i nowych wersji oprogramowania przez minimum 3 lat	TAK	
System musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego systemu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z systemem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

6. **Szczegółowa specyfikacja techniczna proponowanego systemu zarządzania siecią – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

TREŚĆ WYMAGANIA	*Wymagane minimalne parametry*	*Oferowane*
Producent, numer produktu, kraj pochodzenia		
Oferowany system musi pochodzi od tego samego producenta co oferowane urządzenia typu przełącznik główny, przełączniki dostępowe, system zapór ogniowych oraz urządzenie na styku z Internetem w celu zapewnienia jak najlepszej integracji i wykorzystaniu jak największej ilości funkcjonalności oferowanych przez taki system	TAK	
Pełna kompatybilność wymaganych funkcjonalności z oferowanymi urządzeniami typu przełącznik główny, przełączniki dostępowe, system zapór ogniowych oraz urządzenie na styku z Internetem	TAK	
Obsługa minimum 60 urządzeń sieciowych, w tym urządzeń dostarczonych w ramach niniejszego postępowania. Możliwość rozbudowy systemu do min. 500 urządzeń	TAK	
Dostarczone licencje na ilość obsługiwanych urządzeń sieciowych muszą być bezterminowe	TAK	
Wymagana jest architektura serwer-klient z dostępem do systemu przez przeglądarkę WWW	TAK	
Wymagany interfejs użytkownika w języku polskim lub angielskim	TAK	
Obsługiwana lokalna baza administratorów systemu	TAK	
Czasowe blokowanie możliwości logowania użytkownika systemu w przypadku 5-krotnego podania błędnego hasła	TAK	
Możliwość stworzenia kopii zapasowej danych systemu zarządzania i odtworzenia tych danych z kopii	TAK	
W przypadku, gdy oprogramowanie korzysta z systemu licencjonowania powinna być zapewniona możliwość sprawdzenia zainstalowanej licencji oraz zmiany licencji	TAK	
Monitorowanie wykorzystania licencji i informowanie użytkownika systemu o zbliżającej się dacie wygasania licencji, bądź przekroczenia limitów zainstalowanej licencji (np. Ilość obsługiwanych urządzeń)	TAK	
Dostępna w systemie zarządzającym dokumentacja w języku polskim lub angielskim	TAK	
Możliwość automatycznego alarmowania opartego o zadane progi alarmowe	TAK	
Możliwość definiowania dwóch progów – ostrzegawczy i alarmowy	TAK	
Możliwość automatycznego alarmowania opartego o profil ruchu	TAK	
Możliwość automatycznego alarmowania o przekroczeniu obciążenia interfejsu z uwzględnienie dwóch progów - ostrzegawczy i alarmowy	TAK	
Możliwość określenia listy osób i grup osób powiadamianych przy poszczególnych poziomach alertów	TAK	
Możliwość wykorzystania następujących kanałów powiadomienia dla poszczególnych poziomów alarmów - konsola operatora	TAK	

- e-mail		
Zapisywanie informacji o czynnościach wykonanych przez użytkowników systemu	TAK	
Możliwość przeszukiwania dziennika czynności pod kątem użytkownika, adresu IP, z którego nastąpiło logowanie, czasu i rodzaju czynności	TAK	
Zapisywanie informacji o zdarzeniach systemowych	TAK	
Możliwość przeszukiwania dziennika zdarzeń systemowych pod kątem czasu i rodzaju zdarzenia	TAK	
Podstawowe zarządzanie wszelkimi urządzeniami zgodnymi z protokołem SNMP	TAK	
Możliwość ręcznego dodania urządzenia poprzez podanie jego adresu IP i parametrów SNMP i telnet	TAK	
Automatyczne wyszukiwanie i dodawanie urządzeń w ramach zdefiniowanego zakresu adresów IP	TAK	
Możliwość importowania listy urządzeń z pliku	TAK	
Możliwość podglądu podstawowych informacji o urządzeniu	TAK	
Możliwość wizualizowania panelu urządzenia	TAK	
Możliwość wyświetlenia listy interfejsów urządzenia i włączenia/wyłączenia poszczególnych interfejsów	TAK	
Wyświetlanie adresu IP urządzenia	TAK	
Możliwość zdefiniowania parametrów SNMP i telnet dla danego urządzenia	TAK	
Możliwość przeprowadzenia testów ping i traceroute dla wybranego urządzenia	TAK	
Zapewnienie skrótu do wyświetlenia listów alarmów i konfiguracji urządzenia	TAK	
Możliwość zdefiniowania skrótów do funkcji dla urządzeń nieznanych producentów	TAK	
Możliwość zdefiniowania podstawowych informacji o dowolnym producencie urządzeń, w celu ułatwienia definiowania nowych elementów sieciowych nieobsługiwanych domyślnie przez system zarządzania	TAK	
Możliwość dodawania, kasowania i modyfikacji nowych typów urządzeń.	TAK	
Możliwość określenia ikony reprezentującej urządzenie w systemie	TAK	
Możliwość zdefiniowania skrótów funkcyjnych skojarzonych z nowym typem urządzenia	TAK	
Możliwość definiowania nowych typów alarmów nierozpoznawanych domyślnie przez system zarządzania	TAK	
Możliwość definiowania nowych typów liczników danych, ich nazwy, funkcji obliczającej wartość licznika i rodzajów urządzeń, dla których dany licznik może zostać zastosowany	TAK	
Możliwość tworzenia kopii zapasowych konfiguracji urządzeń oraz odtwarzania zapisanej konfiguracji	TAK	
Możliwość definiowania wyglądu panela urządzenia przy użyciu rysunków urządzenia, modułów i portów	TAK	
Wyświetlanie topologii sieci z urządzeniami i łączami pomiędzy nimi	TAK	
Możliwość powiększania i zmniejszania widoku topologii	TAK	
Obrazowanie statusu dostępności urządzeń i łączy	TAK	

Możliwość zdefiniowania obrazu tła dla mapy topologii sieci	TAK	
Możliwość zdefiniowania różnych lokalizacji na mapie sieci	TAK	
Zbieranie alarmów i zdarzeń w dzienniku zdarzeń	TAK	
Możliwość wyświetlenia informacji o alarmach, nazwy, źródła, poziomu alarmu, czasu wystąpienia	TAK	
Możliwość potwierdzenia alarmu przez użytkownika, możliwość wyłączenia alarmu	TAK	
Możliwość eksportu danych o alarmach do pliku	TAK	
Możliwość wyświetlenia historii alarmów zawierającej nazwę alarmu, jego źródło, poziom, status i czas wygenerowania. Możliwość filtrowania wyświetlanej listy przy pomocy powyżej podanych parametrów	TAK	
Możliwość podjerzenia alarmów wygenerowanych na podstawie kilku innych alarmów z tego samego źródła	TAK	
Możliwość zdefiniowania reguł ignorowania alarmów	TAK	
Możliwość generowania powiadomienia o alarmach w postaci email i SMS	TAK	
Możliwość zdefiniowania reguł powiadamiania	TAK	
Monitorowanie obciążenia procesora i zajętości pamięci urządzenia, stanu dostępności urządzenia i opóźnienia	TAK	
Możliwość monitorowania informacji o przesyłanym przez urządzenie ruchu	TAK	
Możliwość generowania alarmu w przypadku przekroczenia zdefiniowanych wartości	TAK	
Możliwość przechowywania historycznych danych wydajnościowych z ostatnich 30 dni	TAK	
Możliwość obrazowania danych historycznych na wykresach	TAK	
Możliwość eksportu danych historycznych do pliku	TAK	
Automatyczne wyszukiwanie łączy przy wykorzystaniu informacji dostępu z protokołu LLDP oraz z adresacji IP	TAK	
Możliwość generowania raportów na temat urządzeń, modułów, portów i łączy oraz statystyk nt. rodzajów urządzeń	TAK	
Możliwość generowania raportów wydajnościowych dotyczących urządzeń oraz ich interfejsów	TAK	
Możliwość tworzenia, wyświetlania, edytowania i kasowania zadań raportowych	TAK	
Możliwość udostępnienia raportów użytkownikom do podglądu oraz do eksportu do pliku	TAK	
Możliwość automatycznego generowania raportów w cyklach: dziennym, tygodniowym, miesięcznym, kwartalnym, półrocznym i rocznym	TAK	
Możliwość generowania raportów w formatach PDF	TAK	
Możliwość generowania raportów w formatach Excel, Word, PowerPoint użytkowanych przez Zamawiajacego	TAK	
Możliwość definiowania szablonu określającego wygląd raportów	TAK	
Możliwość automatycznego wykonywania w określonym czasie kopii zapasowych konfiguracji urządzeń w trybie dziennym, tygodniowym i miesięcznym	TAK	
Możliwość podglądu i porównania różnych wersji plików konfiguracyjnych, w tym z aktualną konfiguracją urządzenia	TAK	
Możliwość konfiguracji urządzeń, w tym list kontroli dostępu, ustawień QoS, VLAN, poprzez wysłanie szablonów	TAK	

konfiguracyjnych do wielu urządzeń		
Możliwość definiowania ww. szablonów konfiguracyjnych	TAK	
System musi być dostarczony wraz z platformą serwerową tego samego producenta co oprogramowanie, o parametrach spełniających wymagania specyfikacji rekomendowanej przez producenta systemu dla min. 60 urządzeń sieciowych i jednocześnie spełniających następujące minimalne wymagania: - obudowa przeznaczona do montażu w szafie 19” - maksymalna wysokość 2RU - 8 GB RAM - 2 procesory sześciordzeniowe min. 2.5GHz - min. 2 dyski 300GB SAS hotswap - sprzętowy kontroler RAID 0,1,5,10 - 4 interfejsy sieciowe GigabitEthernet - 5 slotów PCIe - 2 redundantne zasilacze - minimum 2 porty USB - niezależny od CPU kontroler zdalnego zarządzania serwerem z funkcją zdalnego restartu oraz zdalnej konsoli wspierającej systemy operacyjne z rodziny Linux, Windows. Jeżeli dla funkcjonalności zdalnego zarządzania wymagana jest licencja, zostanie ona dostarczona przez Wykonawcę	TAK	
Oprogramowanie do zarządzania siecią należy dostarczyć wraz z serwisem gwarancyjnym na minimum 3 lat.	TAK	
Serwis ten musi zapewniać dostęp do zdalnego wsparcia technicznego producenta przez całą dobę, 7 dni w tygodniu	TAK	
Serwis musi zapewniać bezpłatny dostęp do poprawek i nowych wersji oprogramowania przez minimum 3 lat	TAK	
System musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego systemu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z systemem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

7. **Szczegółowa specyfikacja techniczna proponowanego serwera - 2 Kpl. – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

TREŚĆ WYMAGANIA	**Wymagane minimalne parametry**	**Oferowane**
Producent, typ produktu, model (podać)		
Maksymalnie 2U do instalacji w standardowej szafie RACK 19”, dostarczona wraz z szynami	TAK	
Płyta główna z możliwością zainstalowania do dwóch procesorów, wspierających od 4 do 12 rdzeni. Obsługa procesorów o mocy do 130W. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym	TAK	
Dwa procesory ośmiordzeniowy klasy x86 dedykowany do pracy w serwerach zaprojektowany do pracy w układach dwuprocesorowych, taktowany zegarem co najmniej 2,6 GHz, pamięć L3 20MB TDP maksymalnie 95W lub procesory równoważne wydajnościowo. W przypadku procesorów równoważnych, oferowany model serwera z procesorem równoważnym musi osiągać w teście dla maszyn dwu procesorowych SPECint_rate2006 wynik minimum 682 pkt. w konfiguracji 2 procesory / 16 rdzeni (tj. 8 rdzenie na procesor). Wyniki testu muszą być opublikowane i powszechnie dostępne na stronie www.spec.org	TAK	
Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	TAK	
128GB DDR3 RDIMM 1600MHz, płyta powinna umożliwiać instalację minimum 768GB, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych dla pamięci, możliwość instalacji kości taktowanych prędkością 1333MHz,1600MHz,1866MHz pamięci RDIMM, UDIMM, LRDIMM,HCDIMM.	TAK	
ECC, Chipkill, Memory Mirroring, Memory rank sparing	TAK	
Minimum 3 sloty PCIe x8 trzeciej generacji ,w tym min jeden slot x8 pełnej wysokości i długości. Możliwość rozbudowy o kolejne trzy sloty PCIe x8 lub dwa sloty PCIe jeden x16 drugi x8	TAK	
Minimum 4 interfejsy LAN typu 10/100/1000mb wbudowane na płycie głównej Karty sieciowe powinny wspierać: - TCP Offload Engine (TOE) - Wake on LAN suport - 802.1Q VLAN tagging - NIC Teaming (Load Balancing and Failover, Zamontowana dodatkowa karta Ethernet dwu portowa 10/100/1000mb Możliwość zamontowania dwu portowej karty 10Gb z gniazdami SFP+ lub RJ45,posiadającej swoje dedykowane złącze na płycie głównej, nie zajmującej żadnego ze slotów PCI-e,	TAK	

Możliwość instalacji dysków SATA, SAS, SSD. Obsługa do 16 dysków twardych typu: SAS, SATA, SSD	TAK	
Możliwość zamontowania DVD-ROM wewnątrz obudowy serwera Możliwość zamontowania wewnątrz obudowy serwera, napędu RDX	TAK	
Dedykowany kontroler RAID wbudowany na płycie głównej. Możliwe konfiguracje 0, 1, 10, 5, 50. Możliwość rozbudowy wbudowanego w płytę kontrolera dyskowego o dodatkowe funkcje, takie jak RAID 6, 60,Kontroler musi posiadać 1GB nieulotnej pamięci Flash	TAK	
8 portów USB 2.0 z czego 2 na przednim panelu obudowy, 4 na tylnym panelu obudowy i 2 wewnątrz obudowy min jeden wewnętrzny port USB służący do podłączenia Hypervisora ESXI - dwa porty VGA (jeden z przodu drugi z tyłu obudowy) -wbudowana karta sieciowa Rj45 4 portowa - Dodatkowy niezależny port RJ45 przeznaczony do zarządzania serwerem -jeden serial port	TAK	
Zintegrowana karta graficzna 16M, o rozdzielczości min. 1600x1200. 75Hz z 16M color	TAK	
Dwie dwuportowe karty 6Gb SAS HBA	TAK	
Panel diagnostyczny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o: - stanie procesora - pamięciach - dyskach - logach - slotach PCI - zasilaczach - temperaturze.	TAK	
Dwa Redundantne zasilacze o maksymalnym poborze 750W każdy, posiadający certyfikat 80 Plus Platinum	TAK	
Standardowo serwer musi posiadać kartę zarządzającą umożliwiającą: - dostęp do konsoli zarządzającej musi odbywać się za pomocą osobnego, dedykowanego porty RJ45 lub za pomocą udostępnionego portu ethernet z niezależnym portem RJ45 umożliwiającą : - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera - integracja z Active Directory - wsparcie dla IPv6 - wsparcie DHCP - wsparcie serwera DNS - wsparcie dla DDNS - wsparcie dla IPMI 2.0,CIM oraz SNMP - zdalne włączanie i wyłączanie serwera - możliwość obsługi przez dwóch administratorów jednocześnie	TAK	

- Automatyczne wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej - dziennik zdarzeń z możliwością przesyłania drogą meilową - zdalne uaktualnienie firmware - uwierzytelnianie użytkowników za pomocą LDAP - zdalne przejęcie konsoli graficznej w rozdzielczości 1600x1200 - zdalny dostęp za pomocą klawiatury i myszy - mapowanie dysków cd,dvd,dyskietki i pamięci flash usb na zdalnym serwerze, mapowanie ISO i obrazów dyskietek jako wirtualnych napędów, które będą dostępne i wykorzystywane przez serwer - Przechwytywanie blue-screen i możliwość podglądu ich przed ponownym restartem		
- Microsoft Windows Server 2008,2008 R2 ,2012 - Red Hat Enterprise Linux 5 and 6, - SUSE Linux Enterprise Server 10 and 11, - VMware ESX 4.1 and VMware ESXi 4.1 VMware vSphere 5,1 - Solaris 10 Operating System	TAK	
Dostarczony Hypervisor -pamięć USB z VMware ESXI 5.1	TAK	
Gwarancja 3 lata świadczona minimum 7 dni w tygodniu przez minimum 24 godzin w ciągu doby Gwarantowany czas naprawy serwera 24 godziny	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

8. **Szczegółowa specyfikacja techniczna proponowanego oprogramowania dla serwera – 2 sztuki – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

Oprogramowanie dla serwera	**Wymagane minimalne parametry**	**Oferowane**
Producent, typ produktu, model (podać)		
Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Serwerowy system operacyjny (SSO) typ II musi posiadać następujące, wbudowane cechy:	TAK	
Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym	TAK	
Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.	TAK	
Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.	TAK	
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.	TAK	
Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.	TAK	
Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.	TAK	
Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.	TAK	
Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.	TAK	
Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,	TAK	

d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).		
Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.	TAK	
Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.	TAK	
Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET	TAK	
Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.	TAK	
Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.	TAK	
Graficzny interfejs użytkownika.	TAK	
Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,	TAK	
Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.	TAK	
Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).	TAK	
Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.	TAK	
Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.	TAK	
Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).	TAK	
Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 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: i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala	TAK	

(cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw trunk mode)		
Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.	TAK	
Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).	TAK	
Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.	TAK	
Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	TAK	

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.	TAK	
Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.	TAK	
Licencja zapewniająca możliwość równoczesnego dostępu do zasobów serwera przez 100 urządzeń/stacji roboczych.	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

9. Szczegółowa specyfikacja techniczna proponowanej platformy pamięci masowej – 1 Kpl. – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, typ produktu, model (podać)		
Wymagane jest niemniej niż: - 2 porty 1Gb Ethernet w każdym kontrolerze do podłączenia hostów - 1 port SAS do podłączenia dodatkowych półek dyskowych w każdym kontrolerze - 7 porty SAS w każdym kontrolerze do podłączenia hostów Macierz musi zapewniać możliwość wymiany karty rozszerzeń w każdym z kontrolerów na jedną z następujących kart: 4 porty x 1Gb/s Ethernet (iSCSI) 2 porty x 10Gb/s Ethernet (iSCSI/FCoE) 4 porty x 8 Gb/s FC	TAK	
Graficzny interfejs przez przeglądarkę, oraz interfejs tekstowy przez ssh	TAK	
Kontroler podwójny Active-Active z funkcją Mirrored cache	TAK	
Macierz musi być wyposażona w minimum 4GB pamięci Cache na kontroler. Musi istnieć możliwość rozbudowy do 8GB pamięci cache na kontroler Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.	TAK	
Wymagane jest dostarczenie dodatkowej półki dyskowej na 24 dyski 2,5” i półki dyskowej na dodatkowe 12 dysków 3,5” Należy dostarczyć wszystkie kable SAS do połączenie dwóch półek dyskowych z kontrolerem Wymaga się dostarczenia ośmiu kabli SAS do podłączenia macierzy z serwerami	TAK	
- 7 dysków 146GB 15K rpm 2,5”SAS - 17 dysków 300GB 10K rpm 2,5’’ SAS - 7 dysków 3TB 7,2K rpm 3,5” NL SAS	TAK	
Macierz musi obsługiwać półki zdyskami 2,5” jak i 3,5”. muszą obsługiwać dyski 2,5”o pojemnościach i prędkościach: - 146GB 15k, 300GB 15k, SAS - 300GB 10k, 600GB 10k 900GB 10k, 1,2TB SAS - 500GB 7,2k, 1TB 7,2k NLSAS - 200GB SSD, 400GB SSD, 800GB SSD Półki 3,5’’ 12 dyskowe muszą obsługiwać dyski 3,5”o pojemnościach i prędkościach - 2TB 7,2k 3TB 7,2k NLSAS 4TB 7,2k NLSAS - 300GB 15K, 900GB 10k, 1,2TB SAS Macierz musi obsługiwać dyski SSD i SAS, NLSAS	TAK	

Macierz musi obsługiwać co najmniej 120 dysków 2,5”lub 60 dysków 3,5” na parę kontrolerów		
RAID 0, 1, 5, 6 i 10	TAK	
W pełni nadmiarowe, z możliwością wymiany podczas pracy	TAK	
Standardowy stelaż 19-calowy	TAK	
Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.	TAK	
- wirtualizacja wewnętrznych zasobów dyskowych - macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.. - jednokierunkowa migracja danych i funkcje kopiujące typu migawka i klon (maksymalnie 64 cele, z możliwością rozbudowy do co najmniej 2000) - kopie danych typu PIT musza być tworzone w trybach incremental, multitarget, oraz kopii pełnej , kopii wskaźników - macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji - musi istnieć możliwość migracji danych z macierzy innych producentów za pomocą kontrolerów; kopiowanie danych z migorwanego systemu musi odbywać się w sposób przezroczysty dla aplikacji, bez przerywania pracy systemu - Macierz musi posiadać funkcjonalność tworzenia mirrorowanych LUN pomiędzy różnymi zarządzanymi zasobami dyskowymi w szczególności na różnych poziomach RAID, z zastosowaniem innych dysków w grupach dyskowych, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować, dla maksymalnej pojemności macierzy i maksymalnej liczby wolumenów - macierz musi obsługiwać LUN Masking i Lun mapping - Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych - minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) musi wynosić co najmniej 2048 - wymienione funkcjonalności muszą być dostarczone.	TAK	
• 3-letnia gwarancja • Zgłaszanie przyjmowane 24 godziny na dobę 7 dni w tygodniu • Gwarantowany czas naprawy 24 godziny Macierz musi pochodzić z autoryzowanego kanału dystrybucji producenta i być objęta serwisem producenta na terenie RP	TAK	
Główna jednostka z dyskami – max 360W, napięcie 100-240V	TAK	
Macierz musi posiadać możliwość rozbudowy o następujące funkcjonalności: - Optymalizacja wykorzystania dysków SSD poprzez automatyczną	TAK	

identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migracje na dyski SSD. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD i automatycznie migrować z dysków SSD nieobciążone fragmenty wolumenów. Opisany powyżej proces optymalizacji musi posiadać funkcję właczenia/wyłączenia na poziomie pojedynczego wolumenu. - Wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych		
Apple MacOSX 10.5, Debian, HP-UX, IBM AIX 5.3/6.1/7.1, Microsoft Windows 2003/2008/2008R2/2012, Suse 10/11, Redhat 5/6, Solaris 9/10, VMware 4.1/5.0/5.1	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

10. Szczegółowa specyfikacja techniczna proponowanego systemu kopii zapasowych – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	*Wymagane minimalne parametry*	*Oferowane*
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia centralnego systemu do backupu serwerów systemów otwartych (UNIX/Linux/Windows), w tym również a. działających w środowisku wirtualnym b. działających w zdalnych oddziałach oraz laptopów połączonych z centralą siecią GSM.	TAK	
Oferowany system musi tworzyć centralny system backupu wykonujący kopie zapasowe oraz zapewniać przechowywanie wszystkich zdeduplikowanych kopii zapasowych na własnych dyskach.	TAK	
Wymagane jest dostarczenie urządzenia do przechowywania backupów jak również oprogramowania backupowego tworzącego łącznie jedną logiczną całość (appliance składający się z sprzętu i oprogramowania) stanowiącego kompletny system centralnego backupu z agentami do backupu plików, baz danych, środowisk vmware, HyperV oraz zawierającego medium backupowe w dostarczonym urządzeniu. Oprogramowanie i sprzęt musi pochodzić od jednego producenta	TAK	
W ramach dostawy wymagane jest dostarczenie urządzenia z przestrzenią dyskową zapewniającą przechowywanie zdeduplikowanych danych o łącznej pojemności przynajmniej 3,9 TB de-duplikatów oraz licencji na przechowywanie minimum 2TB de-duplikatów	TAK	
W ramach projektu wymagane jest dostarczenie usług wdrożeniowych obejmujących również dokumentację	TAK	
Dostarczony system musi przechowywać kopie zapasowe na własnych dyskach wewnętrznych. Nie dopuszcza się przechowywania danych na taśmach magnetycznych czy tez zabezpieczanych maszynach	TAK	
Zainstalowany w urządzeniu system centralnego backupu musi być dostarczony z licencją na nielimitowaną liczbę zabezpieczanych serwerów / systemów operacyjnych / baz danych / partycji VMWare / partycji HyperV / laptopów	TAK	
Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu), Solaris, AIX, HP-UX, Mac OS X, NetWare, Novell OES 2, FreeBSD. Backup zasobów plików z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami powyżej.	TAK	

Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange (2007, 2010), MS SQL, Oracle, IBM DB2, Lotus Notes, SharePoint, SAP, Sybase, VMware, HyperV. Backup z powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami zawartymi w niniejszym dokumencie.	TAK	
W przypadku zabezpieczania baz danych i aplikacji musi istnieć możliwość pobierania kopii zapasowej kilkoma strumieniami jednocześnie (minimum 5 jednoczesnych strumieni).	TAK	
W przypadku zabezpieczania systemu Exchange 2010 musi istnieć możliwość backupu całego obrazu bazy danych i jednocześnie odtworzenia pojedynczego maila bez konieczności odtwarzania całej bazy danych.	TAK	
W przypadku zabezpieczania systemu Sharepoint musi istnieć opcjonalna (licencja nie jest wymagana) możliwość odtworzenia pojedynczego elementu systemu Sharepoint bez konieczności odtwarzania całego środowiska SharePoint	TAK	
Oferowane rozwiązanie musi zabezpieczać zde-duplikowane dane Windows 2012 bez konieczności przywracania danych Windows 2012 do postaci oryginalnej (nie zde-duplikowanej).	TAK	
Zabezpieczane serwery muszą być backupowane bezpośrednio na medium backupowe (dyski oferowanego applaince'u) bez pośrednictwa jakichkolwiek innych urządzeń / serwerów. Dotyczy to backupów lokalnych, zdalnych jak również backupu laptopów	TAK	
Transfer danych z zabezpieczanych serwerów do oferowanego appliance'u backupowego nie może się odbywać po sieci SAN.	TAK	
Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej: c. backup pojedynczych plików d. backup całych systemów plików e. backup baz danych w trakcie ich normalnej pracy f. backup ustawień systemu operacyjnego Windows. g. backup całych obrazów maszyn wirtualnych systemu VMWare • *backup całych obrazów maszyn wirtualnych systemu HyperV*	TAK	
Rozwiązanie backupowe musi transferować dane bezpośrednio z ze zdalnych oddziałów do appliance'u backupowego bez konieczności instalacji jakiegokolwiek sprzętu w oddziale. Backup zdalnych oddziałów musi działać poprawnie nawet w przypadku opóźnienia 2 sekund w sieci WAN oraz jednocześnie utraty pakietów na poziomie 60%. Powyższa funkcjonalność wymagana jest dla następujących typów danych: h. backup pojedynczych plików i. backup całych systemów plików • backup baz danych w trakcie ich normalnej pracy	TAK	
Rozwiązanie backupowe nie może wymagać jakichkolwiek czynności ze strony personelu w oddziale. Rozwiązanie backupowe musi działać zakładając, że pracownicy oddziału nie wiedzą w ogóle o istnieniu rozwiązania backupowego.	TAK	
Rozwiązanie backupowe musi być w pełni konfigurowalne z konsoli znajdującej się w centrali. W szczególności backupy maszyn w	TAK	

oddziałach (bazy, pliki) czy też backupy laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.		
Rozwiązanie backupowe musi mieć możliwość odtworzenia j. plików k. baz danych na docelowa maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.	TAK	
W przypadku odtwarzania systemu plików rozwiązanie backupowe musi mieć możliwość odtworzenia tylko brakujących lub uszkodzonych plików. Pliki które są identyczne na odtwarzanej maszynie oraz w backupie nie mogą być odczytane z systemu backupowego i transferowane na odtwarzaną maszynę.	TAK	
Oferowane rozwiązanie musi być odporne na: l. Opóźnienia na łączu między oddziałem a ośrodkiem regionalnym (do 2s) m. Zrywanie łącza między oddziałem a ośrodkiem regionalnym (do 1h) • Utraty pakietów (60%)	TAK	
Oprogramowanie backupowe musi mieć funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu. Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.	TAK	
Oprogramowanie backupowe musi backupować (przesyłać do serwera backupu) tylko unikalne bloki w skali całego zabezpieczanego środowiska skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN. Fragment danych, których został przesłany z serwera A nie może być przesłany nigdy więcej z żadnego innego serwera znajdującego się w jakimkolwiek oddziale.	TAK	
Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany, chyba, że zmieni się jego zawartość.	TAK	
Oprogramowanie backupowe musi wykonywać logicznie pełne backupy systemu plików. W wewnętrznej strukturze musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach). Odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.	TAK	
Oferowane oprogramowanie musi samodzielnie i automatycznie zarządzać mediami (wewnętrznymi dyskami) na których przechowuje backupy. Administrator musi być uwolniony od jakichkolwiek czynności związanych z definicją mediów, przyporządkowaniem mediów do zadań backupowych, definiowaniem gdzie przechowywane są zadania backupowe. Wszystkie te czynności, oferowane rozwiązanie musi wykonywać	TAK	

samodzielnie i automatycznie bez jakiegokolwiek angażowania administratora. Jedynym wyjątkiem alternatywne wskazanie dodatkowego de-duplikatora jako medium dla danego zadania backupowego		
W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.	TAK	
Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu Dziadek – ojciec –syn, to znaczy utworzenia polityki w której zdefiniowano: n. Czas przechowywania backupów dziennych o. Czas przechowywania backupów tygodniowych p. Czas przechowywania backupów miesięcznych • Czas przechowywania backupów rocznych	TAK	
Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów: q. wybranych typów plików, np. dla plików z rozszerzeniem mp3 r. dla całych katalogów (np.: c:\windows). • dla pojedynczych plików	TAK	
Niezależnie od dostarczonego urządzenia (appliance fizyczny) musi istnieć możliwość (przyszła rozbudowa) zainstalowania analogicznego serwera backupu na platformie VMware ESX (appliance wirtualny). Urządzenia podstawowe (będące przedmiotem przetargu) jak również przyszłościowa platforma zainstalowana na VMware w ośrodku zdalnym musza mieć możliwość replikacji danych w obu kierunkach jednocześnie: s. appliance fizyczny do appliance wirtualny t. appliance wirtualny do appliance fizyczny Replikacji powinny podlegać tylko bloki unikalne, nieznajdujące się na docelowym urządzeniu. Musi istnieć możliwość zdefiniowania kalendarza replikacji między appliance'mi oraz zdefiniowania które zadania backupowe podlegają replikacji.	TAK	
Oferowane rozwiązanie musi zapewniać repliakcję danych do centrum zapasowego na identyczne z dostarczanym urządzeniem, z zachowaniem funkcjonalności powyżej.	TAK	
Oferowane urządzenie musi mieć możliwość rozbudowy poprzez dokładanie analogicznych serwerów do farmy serwerów przy zapewnieniu następującej funkcjonalności: 1. Farma serwerów posiada wspólną bazę de-duplkatów rozciągniętą na wszystkie node'y farmy 2. Awaria pojedynczego serwera w ramach farmy nie powoduje utraty danych (bazy de-duplikatów) ani też przerwy w pracy systemu backupowego 3. Każdy z serwerów powinien mieć zabezpieczenie RAID dla przechowywanych de-duplikatów 4. Wszystkie serwery farmy są w stanie jednocześnie przyjmować strumień backupów (de-duplikatów od zabezpieczanych serwerów) / odtwarzać dane 5. System dba by każdy z węzłów farmy był równomiernie	TAK	

obciążony przechowywanymi backupami oraz wykonywanymi zadaniami backupowymi oraz odtworzeniowymi. 6. Farma serwerów musi być rozbudowywalna by być w stanie pomieścić bazę de-dupliaktów o łącznej wielkości **minimum 50TB**. 7. Farma serwerów powinna zarządzana poziomu pojedynczej konsoli iw dziana jako pojedyncze logiczne urządzenie Dołożenie kolejnego urządzenia/serwera zwiększa zarówno pojemność systemu jak również wydajność.		
Musi istnieć pojedyncza konsola zarządzająca całym środowiskiem backupowym w ramach pojedynczego applaince'u backupowego (danego ośrodka). Konsola powinna musi mieć możliwość pracy na systemach zarówno Windows jak i Linux.	TAK	
Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról w systemie backupowym.	TAK	
Konsola powinna udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na de-duplikaty.	TAK	
Bloki przesyłane z zabezpieczanych serwerów do appliance'a backupowego muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.	TAK	
Musi istnieć możliwość szyfrowania danych na medium dyskowym przechowującym backupy (de-duplikaty). Ewentualna licencja szyfrowania musi być dostarczona w ramach postępowania.	TAK	
Wymagana jest autentyfikacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach.	TAK	
Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.	TAK	
Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych	TAK	
Oprogramowanie backupowe musi umożliwiać ograniczenie pasma zużytego na przesłanie danych z zabezpieczanej maszyny.	TAK	
Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań.	TAK	
Rozwiązanie backupowe musi wspierać VMware 5.0 oraz 5.1. Oprogramowanie backupowe musi umożliwiać dla środowisk VMware: a. Backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej VMware. b. Backup całych maszyn wirtualnych (obrazów, plików vmdk reprezentujących wirtualną maszynę). W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMWare (wumagane wykorzystanie mechanizmu CBT systemu VMWare) c. Backup tylko wybranych dysków maszyny wirtualnej	TAK	

(wybranych plików vmdk systemu vmware) d. Wykonywanie backupu jak w punkcie b. i c. nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk). e. Wykonywanie backupu jak w punkcie b. musi pozwalać na szybkie odtworzenie 1.całych obrazów maszyn wirtualnych 2.pojedynczych dysków maszyny wirtualnej f. Odtworzenie zarówno całych maszyn wirtualnych jak i pojedynczych dysków musi wykorzystywać mechanizm CBT systemu VMWare – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu g. Wykonywanie backupu jak w punkcie b.i c. musi pozwalać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux. 1. Dopuszcza się wykonywanie snapshotów maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych. 2. Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. 3. Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.		
Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla: u. Folderu v. Hosta ESX w. Resource Pool Systemu VMware Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.	TAK	
Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.	TAK	
Oprogramowanie backupowe musi umożliwiać dla środowisk Hyper-V: a. Backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V. b. Backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę). c. Wykonywanie backupu jak w punkcie b. nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd). d. Wykonywanie backupu jak w punkcie b. musi pozwalać na odtworzenie pojedynczych plików z obrazu maszyny	TAK	

wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows. 1. Dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych. 2. Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. 3. Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.		
Oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazó maszyn wirtualnych środowiska Hyper-V	TAK	
Musi istnieć możliwość odtworzenia danych x. z zabezpieczanego serwera / komputera 4. z konsoli systemu backupowego	TAK	
Musi istnieć możliwość odtworzenia: a. Pojedynczego pliku • Zabezpieczanej bazy danych	TAK	
Dla systemów Windows 2008, Windows 7 musi istnieć funkcjonalność Bare Metal Recovery automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia. Funkcjonalność musi być wbudowana w rozwiązanie backupowe.	TAK	
W przypadku odtwarzania danych z interfejsu dostępnego na zabezpieczanym serwerze musi istnieć mechanizm autentyfikacji użytkowników dostępny w dwóch opcjach: b. Wbudowany w system backupowy c. Zintegrowany z usługami katalogowymi d. W przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności - odtworzenia danych - przeszukania zwartości swoich backupów - wykonania backupu	TAK	
Dla odtwarzania danych z interfejsu końcowego użytkownika dostępnego na zabezpieczanym laptopie / PC muszą być dostarczone następujące funkcjonalności: e. Wyszukiwanie pliku do odtwarzania po - nazwie pliku - początkowym fragmencie nazwy pliku - końcowym fragmencie nazwy pliku - fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku f. Przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia • Wybór wersji odtwarzanego pliku / katalogu	TAK	
W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) musi być możliwość odtworzenia danych w taki sposób, że odtwarzane i przesyłane są	TAK	

tylko brakujące pliki i katalogi. Pliki i katalogi które znajdują się i są poprawne na docelowym systemie nie mogą być odtwarzane z urządzenia backupowego i wysyłane z urządzenia backupowego do docelowej maszyny		
System backupu musi mieć funkcjonalność wyrzutu na taśmę (przyszła rozbudowa) będącą jego integralną częścią. Musi to być gotowy moduł producenta systemu spełniający następujące wymagania g. niewymagający skryptów h. niewymagający dodatkowego oprogramowania poza dostarczonym przez producenta i. zawierający interfejs GUI producenta j. posiadający pełne wsparcie producenta Opcja wyrzutu na taśmę nie jest być elementem niniejszej oferty.	TAK	
System backupu musi być dostępny dla backupu i odtwarzania przez 24h na dobę 7 dni w tygodniu. Nie może być jakiegokolwiek przedziału czasowego czy momentu w którym system backupowy nie może wykonywać backupu lub odtwarzania.	TAK	
System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta	TAK	
System backupu musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie i przyporządkowującego maszynę automatycznie do określonej polityki backupowej.	TAK	
System backupu musi mieć możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta	TAK	
System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu	TAK	
System musi pozwalać na backup serwerów NAS z następującymi funkcjonalnościami: • Z systemu NAS powinny być wysyłane tylko zmienione pliki od ostatniego backupu • W przypadku odtwarzania, uprawnienia użytkowników również są odtwarzane • Integracja z protokołem NDMP systemów NAS Dopuszczalne jest użycie dodatkowego, dedykowanego urządzenia wykonującego de-duplikację systemu NAS.	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

11. Szczegółowa specyfikacja techniczna proponowanego oprogramowania do wirtualizacji parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.	TAK	
Licencje powinny obejmować min. trzy co najmniej dwuprocesorowe serwery.	TAK	
Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone dowolną liczbę rdzeni oraz do 2TB pamięci fizycznej RAM.	TAK	
Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.	TAK	
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-8 procesorowych.	TAK	
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.	TAK	
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.	TAK	
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB.	TAK	
Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.	TAK	
Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.	TAK	
Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.	TAK	
Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES9, SLES8, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris 10,	TAK	

Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 5.1, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04-12.04, SCO OpenServer, SCO Unixware, FreeBSD, Mac OS X 10.7.		
Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji (memory overcommitment).	TAK	
Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy (thin provisioning).	TAK	
Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.	TAK	
Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.	TAK	
Rozwiązanie powinno posiadać zintegrowany system monitoringu, który w razie wystąpienia zdarzenia typu awaria komponentu sprzętowego lub przekroczenie zdefiniowanych parametrów pracy, poinformuje administratora systemu lub wyzwoli trap SNMP.	TAK	
Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.	TAK	
Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.	TAK	
Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory oraz sterowania uprawnieniami w ramach środowiska wirtualnego dla użytkowników Active Directory.	TAK	
Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn.	TAK	
Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.	TAK	
Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.	TAK	
Musi zostać zapewniona odpowiednia redundancja i taki	TAK	

mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.		
System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.	TAK	
Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.	TAK	
Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).	TAK	
Rozwiązanie musi posiadać zintegrowane, dedykowane rozwiązanie do wykonywania kopii bezpieczeństwa. Rozwiązanie powinno wspierać mechanizmy globalnej deduplikacji danych i wykonywać kopie bezpieczeństwa wszystkich uruchomionych w ramach infrastruktury maszyn wirtualnych bez przerwy w ich działaniu.	TAK	
Rozwiązanie musi posiadać zintegrowane rozwiązanie replikacji asynchronicznej maszyn wirtualnych. Mechanizm replikacji powinien umożliwiać przesyłanie jedynie bloków danych zmienionych od momentu ostatniej replikacji (replikacja przyrostowa). Minimalny czas pomiędzy kolejnymi zdarzeniami replikacji powinien wynosić 15 minut. Replikacja danych powinna odbywać z wykorzystaniem sieci LAN lub WAN.	TAK	
Konsola zarządzająca kopiami bezpieczeństwa oraz replikami maszyn wirtualnych powinna być zintegrowania z centralną konsolą do zarządzania środowiskiem wirtualnym.	TAK	
Wparcie producenta oprogramowania na okres 3 lat zapewniające dostęp do aktualizacji oprogramowania oraz zgłaszanie problemów technicznych do wsparcia producenta	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

12. Szczegółowa specyfikacja techniczna proponowanej platformy pracy grupowej – dla 400 użytkowników – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Archiwizacja poczty elektronicznej dla minimalnie 50 użytkowników, możliwość delegacji uprawnień przeszukiwania archiwów.	TAK	
Automatyczne, bezprzerwowe i zintegrowane z konsolą systemu rozwiązanie kopii zapasowych, umożliwiające odtworzenie dowolnej skrzynki (w tym maili, dokumentów i kalendarzy) do punktu w czasie. Punkt w czasie powinien być określony w przeszłości, z precyzją wynoszącą co najmniej 1 sekundę.	TAK	
Możliwość korzystania z systemu, w tym z poczty elektronicznej, wymiany dokumentów czy współdzielenia kalendarzy bez konieczności przechowywania żadnych danych na stacji roboczej.	TAK	
Zintegrowane rozwiązanie AS/AV.	TAK	
Możliwość implementacji w infrastrukturze wirtualnej i uruchomienia funkcjonalności HA.	TAK	
Współdzielenie kalendarzy	TAK	
Współdzielenie poczty elektronicznej	TAK	
Współdzielenie zadań	TAK	
Współdzielenie dokumentów (funkcjonalność aktówki – praca grupowa na dokumentach)	TAK	
Dedykowany i zintegrowany z klientem poczty komunikator internetowy	***TAK***	
Korzystanie z platformy przy wykorzystaniu urządzeń mobilnych (dla minimalnie 50 użytkowników usługa PUSH).	***TAK***	
Wparcie dla następujących systemów operacyjnych z rodziny GNU/Linux: Ubuntu 12.04, SLES 11, RHEL 6, Centos 6.	TAK	
Wsparcie techniczne (subskrypcja) dające prawo do aktualizacji systemu do najnowszej dostępnej wersji przez okres co najmniej 3 lat.	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

13. Szczegółowa specyfikacja techniczna proponowanego komputera (stacji roboczej) typ I – 180 sztuk – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	**Wymagane minimalne *parametry***	***Oferowane***
Producent, numer produktu, kraj pochodzenia (podać)		
Procesor	Zgodny z x64 - dwurdzeniowy, taktowany zegarem co najmniej **3,4** GHz, pamięć cache co najmniej 3 MB lub procesor o równoważnej wydajności osiągający w teście PassMark PerformanceTest co najmniej wynik **4850** punktów PassMark CPU Mark (wynik zaproponowanego procesora musi znajdować sie na stronie http://www.cpubenchmark.net).	
Chipset	Z rodziny Intel H81 – dostosowany do oferowanego procesora lub równoważny.	
Pamięć operacyjna	4GB UDIMM, PC3-12800 1600MHz DDR3 z możliwością rozbudowy do 16 Gb	
Parametry pamięci masowej	500 GB SATA II, 7200 obr./min.	
Karta graficzna	zintegrowana	
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
Obudowa	Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu w tym 1 x PCI Express x 16 oraz 2 x PCIe x 1, 2 kieszenie: 1 szt. 5,25” i 1 szt. 3,5” Suma wymiarów nie może przekroczyć 82 cm. Waga urządzenia nie może przekraczać 6 kg. Zasilacz o mocy 180 W pracujący w sieci 230V 50/60 Hz prądu zmiennego. Obudowa wyposażona w złącze Kensington Lock.	
Zgodność z systemami operacyjnymi i standardami	Oferowany komputer musi być kompatybilny z systemem operacyjnym Windows 8 PRO 64bit.	
Dodatkowe oprogramowanie	Oprogramowanie umożliwiające aktualizacje oprogramowania oraz skanowanie dysku z poziomu podsystemu bezpieczeństwa (nie systemu operacyjnego). Konieczna jest również możliwość dostępu do internetu z poziomu w/w podsystemu. Podsystem ten musi być kompatybilny z MS Active Directory. Oprogramowanie służące do obsługi napędu DVD. Oprogramowanie umożliwiające aktualizacje sterowników oraz podsystemu zabezpieczeń poprzez Internet. Oprogramowanie do wykonania kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku	

	twardym, zewnętrznych dyskach, sieci, CD-ROM-ie oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego reinstalacji. Oprogramowanie w wersji polskiej lub angielskiej Aplikacja umożliwiająca analizę system w celu zdiagnozowania potencjalnych usterek, Aplikacja przechowująca hasła użytkownika. Dostęp do aplikacji za pomocą jednego hasła nadrzędnego.	
Ergonomia	Obudowa w jednostce centralnej musi umożliwiać łatwy demontaż dysku twardego, optycznego oraz pamięci RAM (beznarzędziowe odsłonięcie w/w elementów). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) .Obudowa oraz napęd optyczny muszą umożliwiać prace w pionie oraz poziomie.	
Wymagania dodatkowe	Zainstalowany system operacyjny Windows 8 Professional 64bit PL lub Windows 7 Professional 64bit PL niewymagający aktywacji za pomocą telefonu lub Internetu (lub równoważny). Wbudowane porty: - 2 szt port szerogowy RS232 - 1 szt portów równoległy - 1 szt. VGA; - 1 szt DP; - 6 szt. USB: nie więcej niż 2 x USB2.0 z przodu obudowy, 2 x USB 3.0 i 2 x USB2.0 z tyłu obudowy; - port sieciowy RJ-45; - porty słuchawek i mikrofonu na przednim panelu obudowy; - czytnik kart multimedialnych. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Możliwość podłączenia zewnętrznej karty graficznej. Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL. Płyta główna z wbudowanymi: 1 złączem PCI Express x16; 2 złączami PCI Express x1; 2 złącza DIMM z obsługą do 16GB DDR3 pamięci RAM, 3 złącza SATA (2 x SATAIII, 1 x SATAII). Gniazda PCI wyłącznie o niskim profilu. Dodatkowe złącza portu szeregowego i USB umieszczone na płycie głównej umożliwiające późniejszą rozbudowę. Klawiatura USB w układzie polskim programisty oznaczona trwale logiem producenta komputera. Mysz optyczna USB z klawiszami oraz rolką (scroll) oznaczona trwale logiem producenta komputera. Nagrywarka DVD +/-RW. Opakowanie musi być wykonane z materiałów	

	podlegających powtórnemu przetworzeniu.	
Certyfikaty i standardy	Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-9001 (lub równoważny). Dokument należy załączyć do oferty. Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-14001 (lub równoważny). Dokument należy załączyć do oferty. Deklaracja zgodności CE. Dokument należy załączyć do oferty. Dokument poświadczający, że oferowane stacje robocze spełniają kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (według 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), jak również zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. Dokument należy załączyć do oferty. Deklaracja poświadczająca głośność oferowanej jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO-9296 w pozycji operatora oraz położeniem komputera na biurku w trybie pracy dysku twardego (WORK) wynosi maksymalnie 26 dB. Deklaracja musi zawierać globalne wyniki testów, nie może być lokalnym oświadczeniem producenta spełnienia w/w kryteriów. Dokument należy załączyć do oferty.	
Gwarancja	Minimum 36 miesięcy świadczona w trybie onsite	
Bezpieczeństwo	Hasło użytkownika i administratora w BIOS, HDD password, power-on password	
BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS wraz z datą produkcji, - nr seryjnym komputera wraz z nazwą modelu - informacji Asset Tag - ilości pamięci RAM, - typie procesora wraz z informacją o ilości rdzeni, taktowaniu procesora i pamięci, - modelu i pojemności zainstalowanego dysku twardego, - rodzajach napędów optycznych.	

	- zainstalowaniu wentylatorów Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS). Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. 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 oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego, selektywnego wyłączania napędów SATA z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość selektywnego (pojedynczego) wyłączania portów USB. Możliwość ustawienia stanku komputera po utracie zasilania. Detekcja zmiany konfiguracji systemu na poziomie testu POST Akwizycja zdarzeń systemu np. update Biosu Możliwość zdefiniowania sekwencji botowania z możliwością wykluczenia dowolnego urządzenia z grupy: USB FDD, USB KEY, SATA 1, SATA 2, SATA 3, NETWORK, USB HDD, USB CDROM Obsługa BIOS przy wykorzystaniu klawiatury i myszki.	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

14. Szczegółowa specyfikacja techniczna proponowanego komputera (stacji roboczej) typ II – 2 sztuki – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Procesor	Zgodny z x64 - dwurdzeniowy, taktowany zegarem co najmniej 2,7 GHz, pamięć cache co najmniej 6 MB lub procesor o równoważnej wydajności osiągający w teście PassMark PerformanceTest co najmniej wynik 5800 punktów PassMark CPU Mark (wynik zaproponowanego procesora musi znajdować sie na stronie http://www.cpubenchmark.net).	
Chipset	Z rodziny Intel H81 – dostosowany do oferowanego procesora lub równoważny.	
Pamięć operacyjna	4 GB UDIMM, PC3-12800 1600MHz DDR3 z możliwością rozbudowy do 16 Gb	
Parametry pamięci masowej	1TB SATA II, 7200 obr./min. Dodatkowy dysk ssd min. 180 GB	
Karta graficzna	Zintegrowana Dodatkowa karta graficzna	
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
Obudowa	Typu Mini Tower z obsługą kart PCI Express wyłącznie o pełnym profilu w tym 1 x PCI Express x 16 oraz 2 x PCIe x 1, 3 kieszenie: 1 szt. 5,25” i 2 szt. 3,5” Suma wymiarów nie może przekroczyć 96 cm. Waga urządzenia nie może przekraczać 7,5 kg. Zasilacz o mocy 180 W pracujący w sieci 230V 50/60 Hz prądu zmiennego. Obudowa wyposażona w złącze Kensington Lock.	
Zgodność z systemami operacyjnymi i standardami	Oferowany komputer musi być kompatybilny z systemem operacyjnym Windows 8 PRO 64bit lub Win 7 Pro 64bit	
Dodatkowe oprogramowanie	Oprogramowanie umożliwiające aktualizacje oprogramowania oraz skanowanie dysku z poziomu podsystemu bezpieczeństwa (nie systemu operacyjnego). Konieczna jest również możliwość dostępu do internetu z poziomu w/w podsystemu. Podsystem ten musi być kompatybilny z MS Active Directory. Oprogramowanie służące do obsługi napędu DVD. Oprogramowanie umożliwiające aktualizacje sterowników oraz podsystemu zabezpieczeń poprzez Internet. Oprogramowanie do wykonania kopii bezpieczeństwa	

	systemu operacyjnego i danych użytkownika na dysku twardym, zewnętrznych dyskach, sieci, CD-ROM-ie oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego reinstalacji. Oprogramowanie w wersji polskiej lub angielskiej Aplikacja umożliwiająca analizę system w celu zdiagnozowania potencjalnych usterek, Aplikacja przechowująca hasła użytkownika. Dostęp do aplikacji za pomocą jednego hasła nadrzędnego.	
Ergonomia	Obudowa musi umożliwiać łatwy demontaż dysku twardego, optycznego oraz pamięci RAM. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) .	
Wymagania dodatkowe	Zainstalowany system operacyjny Windows 8 Professional 64bit PL niewymagający aktywacji za pomocą telefonu lub Internetu (lub równoważny). Wbudowane porty: - 2 szt port szerogowy RS232 - 1 szt portów równoległy - 1 szt. VGA; - 1 szt DP; - 6 szt. USB: nie więcej niż 2 x USB2.0 z przodu obudowy, 2 x USB 3.0 i 2 x USB2.0 z tyłu obudowy; - port sieciowy RJ-45; - porty słuchawek i mikrofonu na przednim panelu obudowy; - czytnik kart multimedialnych. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Możliwość podłączenia zewnętrznej karty graficznej. Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL. Płyta główna z wbudowanymi: 1 złączem PCI Express x16; 2 złączami PCI Express x1; 2 złącza DIMM z obsługą do 16GB DDR3 pamięci RAM, 3 złącza SATA (2 x SATAIII, 1 x SATAII). Gniazda PCI wyłącznie pełnym profilu. Klawiatura USB w układzie polskim programisty oznaczona trwale logiem producenta komputera. Mysz optyczna USB z klawiszami oraz rolką (scroll) oznaczona trwale logiem producenta komputera. Nagrywarka DVD +/-RW. Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.	
Certyfikaty i standardy	Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-9001	

	(lub równoważny). Dokument należy załączyć do oferty. Dokument poświadczający, że oferowane stacje robocze produkowane są zgodnie z normą ISO-14001 (lub równoważny). Dokument należy załączyć do oferty. Deklaracja zgodności CE. Dokument należy załączyć do oferty. Dokument poświadczający, że oferowane stacje robocze spełniają kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (według 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), jak również zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. Dokument należy załączyć do oferty. Deklaracja poświadczająca głośność oferowanej jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO-9296 w pozycji operatora oraz położeniem komputera na biurku w trybie pracy dysku twardego (WORK) wynosi maksymalnie 29 dB. Deklaracja musi zawierać globalne wyniki testów, nie może być lokalnym oświadczeniem producenta spełnienia w/w kryteriów. Dokument należy załączyć do oferty.	
Gwarancja	Minimum 36 miesięcy świadczona w trybie onsite	
Bezpieczeństwo	Hasło użytkownika i administratora w BIOS, HDD password, power-on password	
BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS wraz z datą produkcji, - nr seryjnym komputera wraz z nazwą modelu - informacji Asset Tag - ilości pamięci RAM, - typie procesora wraz z informacją o ilości rdzeni, taktowaniu procesora i pamięci, - modelu i pojemności zainstalowanego dysku twardego, - rodzajach napędów optycznych. - zainstalowaniu wentylatorów Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego (gwarantujący utrzymanie zapisanego hasła nawet w przypadku	

	odłączenia wszystkich źródeł zasilania i podtrzymania BIOS). Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. 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 oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego, selektywnego wyłączania napędów SATA z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość selektywnego (pojedynczego) wyłączania portów USB. Możliwość ustawienia stanku komputera po utracie zasilania. Detekcja zmiany konfiguracji systemu na poziomie testu POST Akwizycja zdarzeń systemu np. update Biosu Możliwość zdefiniowania sekwencji botowania z możliwością wykluczenia dowolnego urządzenia z grupy: USB FDD, USB KEY, SATA 1, SATA 2, SATA 3, NETWORK, USB HDD, USB CDROM Obsługa BIOS przy wykorzystaniu klawiatury i myszki.	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

15. Szczegółowa specyfikacja techniczna proponowanego komputera (stacji roboczej) typ III – 5 sztuk – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Ekran	Matryca TFT, 15,6" z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare-rozdzielczość 1920x1080	
Obudowa	Matowa, konstrukcja wzmacniana, zawiasy matrycy metalowe.	
Chipset	Dostosowany do zaoferowanego procesora	
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejsy SATA III (6Gb/s) do obsługi dysków twardych.	
Procesor	Procesor klasy x64, 4 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,2 GHz, pamięcią cache L3 co najmniej 6 MB lub równoważny wydajnościowo osiągający w teście PassMark PerformanceTest co najmniej wynik 7359 punktów PassMark CPU Mark (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net).	
Pamięć operacyjna	Min 8 GB z możliwością rozbudowy do 16GB, rodzaj pamięci DDR3, 1600MHz,	
Dysk twardy	500 gb SSD	
Zabezpieczenie dysku twardego	Komputer wyposażony w czujnik współpracujący z systemem automatycznego parkowania głowicy podczas nagłego upadku komputera	
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,7 GB pamięci. Obsługująca funkcje: • DX10.1 oraz DirectX* 11 on DirectX* 10 hardware • OGL 3.0 • Shader Model 4.1	
Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo, wbudowane dwa mikrofony umożliwiający zmianę charakterystyki kierunkowej zestawu, sterowanie głośnością głośników za pośrednictwem klawiszy funkcyjnych, kamera HD720p pracująca przy niskim oświetleniu z face tracking	
Karta sieciowa	10/100/1000 – RJ 45	
Porty/złącza	2xUSB 3.0, 1xUSB2.0 (dosilone), złącze słuchawek i mikrofonu, VGA, HDMI, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC/MMC)	
Klawiatura	Klawiatura odporna na zalanie, 105 klawiszy, układ US, oraz wbudowanym joystikiem do obsługi	

	wskaźnika myszy, wydzielona sekcja numeryczna	
WiFi	Wbudowana karta sieciowa, pracująca w standardzie a/b/g/n, obsługa Wireless Display-> bezprzewodowa transmisja obrazu w rozdzielczości HD oraz dźwięku 5.1	
Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych wraz z oprogramowaniem działający na poziomie Bios	
Bluetooth	Wbudowany moduł Bluetooth 4.0	
Napęd optyczny	Nagrywarka DVD	
Bateria	Bateria - 6 ogniw 68Whr, pozwalająca na nieprzerwaną pracę urządzenia do 6,2 godziny	
Zasilacz	Zasilacz zewnętrzny max 90W.	
System operacyjny	Microsoft Windows 7 Professional PL 64 bit lub Windows 8 Professional PL 64 bit, zainstalowany System operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft. Dołączony nośnik z oprogramowaniem, sterownikami dla systemów Windows 7, Windows 8 oraz XP, Płyty Recovery umożliwiające reinstalacje systemu. Wraz z systemem operacyjnym zainstalowany pakiet Office Starter.	
BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - wersji BIOS wraz z datą, - nr seryjnym, wersja oraz nazwa komputera - ilości pamięciami RAM - typie procesora, częstotliwości szyny - pojemności zainstalowanego dysku twardego wraz z jego symbolem - rodzajach napędów optycznych wraz z symbolem - MAC Adres karty sieciowej Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) · Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń · 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 oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. · Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcje w BIOS muszą być widoczne lecz bez	

	możliwości modyfikacji. · Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. · 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. **DODATKOWE FUNKCJONALNOŚCI BIOS** - Wake On Lan - Możliwość włączenia/wyłączenia Ethernet LAN Option ROM - Możliwość Wyłączania/Włączania bootowania z USB - Możliwość włączenia/wyłączenia ładowania urządzeń USB podczas uśpienia, hibernacji lub wyłączenia. - Możliwość zamiany funkcje klawiszy FN i Ctrl - Możliwość zdefiniowania podstawowego wyświetlacza Możliwość włączenia/wyłączenia technologii SpeedStep	
Oprogramowanie dodatkowe	Dodatkowe w pełni funkcjonalne oraz nieodpłatne licencyjnie oprogramowanie producenta sprzętu pozwalające na: **Win 7 Pro** - Tworzenie profili użytkownika w zależności od lokalizacji komputera (sieć przewodowa, bezprzewodowa, 3G) - Możliwość ustawienia notebooka w tryb mobilnego accespointa (przy wykorzystaniu modemu 3G) - Automatyczne przełączanie się między profilami w zależności od lokalizacji komputera - Definiowanie w profilu elementów tj.: VPN, uruchamianie dowolnej aplikacji, zmiana drukarki podstawowej włącz/wyłącz firewall, udostępnianie plików, internetu i drukarek, ustawienie serwera proxy i strony domowej, adresu IP - Zdalna implementacji unikatowych profili zaprojektowanych przez administratora sieci na komputerach klienckich - Pokazuje procentowy wskaźnik poziomu sygnału sieci bezprzewodowej - Możliwość tworzenia pliku z wydarzeniami dotyczącymi połączeń sieciowych - Ochrona dysku twardego poprzez parkowanie głowicy dysku przy wykryciu przeciążenie w dowolnej płaszczyźnie - Możliwość włączenia/wyłączenia parkowania głowicy oraz definiowania poziomu czułości systemu ochrony	

	- Samouczący się system bazujący na charakterystykach wcześniejszych przeciążeń - Możliwość backupu metodą: całościową, przyrostową - Asystent Migracji Systemu operacyjnego - Funkcjonalność umożliwiająca transfer danych użytkownika pomiędzy starym a nowym komputerem z wykorzystaniem USB lub LAN - Z miana bilansu wydajność/zużycie energii jednym kliknięciem - Dzienna lub tygodniowa agenda schematu energetycznego (także godzina wyłączenia komputera) - Możliwość zdefiniowania przedziału ładowania baterii (górny i dolny próg) - Informacja o parametrach baterii (poj. Rzeczywista, ilość cykli ładowania, PN, producent) - Narzędzie do automatycznej aktualizacji sterowników i BIOSu komputera Automatyczne blokowanie konta po określonym przez użytkownika czasie odejścia od komputera	
Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty) - Certyfikat EPEAT na poziomie co najmniej GOLD. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony www.epeat.net – ENERGY STAR 5.0 - Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z ww. systemem operacyjnym (załączyć wydruk ze strony Microsoft WHCL) - Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	
Inne	Waga urządzenia z baterią podstawową max 2,5kg, wymiary 377mm x 250mm x 26,9-29,6mm	
Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock Czytnik biometryczny	
Gwarancja	Minimum 36 miesięcy świadczona w trybie onsite	
Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej, możliwość weryfikacji konfiguracji fabrycznej zakupionego sprzętu, a także weryfikacji posiadanej/wykupionej gwarancji oraz statusu napraw urządzenia po podaniu unikalnego numeru seryjnego.	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

16. Szczegółowa specyfikacja techniczna proponowanego monitora typ I – 180 sztuk – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Format ekranu monitora	panoramiczny	
Przekątna ekranu	Min. 19 cali	
Wielkość plamki	0,2835 mm	
Typ panela LCD	TFT LCD	
Technologia podświetlenia	LED Backlight	
Matryca "błyszcząca" (glare)	Nie	
Zalecana rozdzielczość obrazu	1440x900 pikseli	
Czas reakcji matrycy	5 ms	
Jasność	250 cd/m2	
Kontrast	1000:1	
Kąt widzenia poziomy	170 stopni	
Kąt widzenia pionowy	160 stopni	
Certyfikaty	• EPEAT Gold • CE • Energy Star 6.0 • RoHS • TCO 6.0	
Regulacja cyfrowa (OSD)	Tak	
Złącza wejściowe	• 15-stykowe D-Sub • DVI (HDCP)	
Wbudowany zasilacz	Tak	
Pobór mocy	Max. 20 Wat	
Możliwość pochylenia panela (tilt)	Tak	
Montaż na ścianie (VESA)	TAK	
Możliwość zabezpieczenia (Kensington)	Tak	
Kolor obudowy	Czarny	

1.Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2.Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3.Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

17. Szczegółowa specyfikacja techniczna proponowanego monitora typ II – 2 sztuki – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Format ekranu monitora	panoramiczny	
Przekątna ekranu	Min. 21,5 cali	
Wielkość plamki	0,248 mm	
Typ panela LCD	W LED	
Matryca "błyszcząca" (glare)	Nie	
Zalecana rozdzielczość obrazu	1920x1080 pikseli	
Czas reakcji matrycy	5 ms	
Jasność	250 cd/m2	
Kontrast	1000:1	
Kąt widzenia poziomy	170 stopni	
Kąt widzenia pionowy	160 stopni	
Certyfikaty	• EPEAT Gold • CE • Energy Star 6.0 • TCO 6.0	
Regulacja cyfrowa (OSD)	Tak	
Złącza wejściowe	• VGA • HDMI	
Wbudowany zasilacz	Tak	
Pobór mocy	Max. 27 Wat	
Możliwość pochylenia panela (tilt)	Tak	
Montaż na ścianie (VESA)	TAK	
Możliwość zabezpieczenia (Kensington)	Tak	
Kolor obudowy	Czarny	

1.Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2.Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3.Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....
Podpis upełnomocnionego przedstawiciela Wykonawcy

18. **Szczegółowa specyfikacja techniczna proponowanej drukarki (typ I) – 2 sztuki – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Urządzenie fabrycznie nowe, nieużywane	TAK	
Szybkość druku w czerni	20 str./min	
Szybkość druku w kolorze	20 str./min	
Czas wydruku pierwszej strony w czerni i kolorze	17 s.	
Jakość druku w czerni	600 x 600 dpi	
Jakość druku w kolorze	600 x 600 dpi	
Cykl roboczy (miesięcznie, format A4)	40 000 stron	
Technologia druku	Druk laserowy	
Szybkość procesora	600 MHz	
Łączność	• 1 port Hi-Speed USB 2.0 • 1 port sieci Fast Ethernet 10/100Base-TX	
Dostosowany do pracy w sieci	wbudowana karta Fast Ethernet	
Obsługiwane systemy operacyjne	• Pełna instalacja oprogramowania obsługiwana w systemach: Windows 8, Windows 7 (32-bit i 64-bit), Windows Vista (32-bit i 64-bit), Windows XP (32-bit) (wersja SP2 lub wyższa) • Instalacja samego sterownika obsługiwana w systemach: Windows Server 2008 (32-bit i 64-bit), Windows Server 2003 (32-bit) (wersja SP3 lub wyższa) • Mac OS X v10.5, v10.6 • Linpus Linux (9.4, 9.5), Red Hat Enterprise Linux 5.0 (obsługa za pomocą pakietu skonfigurowanego fabrycznie), SuSE Linux (10.3, 11.0, 11, 11.1, 11.2), Fedora (9, 9.0, 10, 10.0, 11.0, 11, 12, 12.0), Ubuntu (8.04, 8.04.1, 8.04.2, 8.10, 9.04, 9.10, 10.04), Debian (5.0, 5.0.1, 5.0.2, 5.0.3) (obsługa za pomocą automatycznego instalatora) • HPUX 11 i Solaris 8/9	
Pojemność podajnika papieru	Podajnik na 50 arkuszy	
Pojemność odbiornika papieru	Odbiornik papieru na 150 arkuszy	

Drukowanie dwustronne	Automatyczny (standardowo)	
Obsługiwane formaty nośników	Podajnik 1: A4, A5, A6, B5 (JIS), 16K, 10 x 15 cm, kartki pocztowe (pojedynczy i podwójny format JIS), koperty (ISO DL, ISO C5, ISO B5); Podajnik 2, opcjonalny podajnik 3: A4, A5, A6, B5 (JIS), 16K, 10 x 15 cm, kartki pocztowe (pojedynczy i podwójny format JIS), koperty (ISO DL, ISO C5, ISO B5); Automatyczny duplekser: A4, B5	
Sprawność energetyczna	• Certyfikat ENERGY STAR® • EPEAT® Bronze	
Zakres temperatur podczas eksploatacji	Od 15 do 30ºC	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

19. Szczegółowa specyfikacja techniczna proponowanej drukarki (typ II) – 47 sztuk – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Automatyczny dupleks	Monochromatyczne, TAK	
Czas wydruku 1 strony	8,5 sek.	
Eksploatacja startowa (w zestawie)	700 str.	
Miesięczne obciążenie	10000 str.	
Procesor	ARM9 200MHz	
Interfejs standardowy	USB 2.0, 10/100 Ethernet Base TX	
Podajnik papieru	250 arkuszy	
Podajnik wielofunkcyjny	1 arkusz	
Poziom hałasu	Drukowanie: 53 dB Stan gotowości: 31 dB	
Prędkość druku	Mono: 26 str./min.	
Rozdzielczość druku	600 x 600 dpi, HQ1200 (2400 x 600 dpi)	
Pamięć (RAM)	32 MB	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

20. Szczegółowa specyfikacja techniczna proponowanego oprogramowania biurowego (typ I) – 85 sztuk – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Edytor tekstów musi umożliwiać:		
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	TAK	
Wstawianie oraz formatowanie tabel	TAK	
Wstawianie oraz formatowanie obiektów graficznych	TAK	
Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)	TAK	
Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków	TAK	
Automatyczne tworzenie spisów treści	TAK	
Formatowanie nagłówków i stopek stron	TAK	
Sprawdzanie pisowni w języku polskim	TAK	
Śledzenie zmian wprowadzonych przez użytkowników	TAK	
Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności	TAK	
Określenie układu strony (pionowa/pozioma)	TAK	
Wydruk dokumentów	TAK	
Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną	TAK	
Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu	TAK	
Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji	TAK	
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.	TAK	
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.	TAK	
Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik	TAK	

wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.		

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

21. Szczegółowa specyfikacja techniczna proponowanego oprogramowania biurowego (typ II) – 102 sztuki – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr 1 do SIWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

TREŚĆ WYMAGANIA	Wymagane minimalne parametry	Oferowane
Producent, numer produktu, kraj pochodzenia (podać)		
Edytor tekstów musi umożliwiać:		
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	TAK	
Wstawianie oraz formatowanie tabel	TAK	
Wstawianie oraz formatowanie obiektów graficznych	TAK	
Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)	TAK	
Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków	TAK	
Automatyczne tworzenie spisów treści	TAK	
Formatowanie nagłówków i stopek stron	TAK	
Sprawdzanie pisowni w języku polskim	TAK	
Śledzenie zmian wprowadzonych przez użytkowników	TAK	
Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności	TAK	
Określenie układu strony (pionowa/pozioma)	TAK	
Wydruk dokumentów	TAK	
Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną	TAK	
Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu	TAK	
Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji	TAK	
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.	TAK	
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.	TAK	
Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i	TAK	

Prawnych.		
Arkusz kalkulacyjny musi umożliwiać:		
Tworzenie raportów tabelarycznych	TAK	
Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych	TAK	
Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.	TAK	
Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)	TAK	
Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych	TAK	
Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych	TAK	
Wyszukiwanie i zamianę danych	TAK	
Wykonywanie analiz danych przy użyciu formatowania warunkowego	TAK	
Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie	TAK	
Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności	TAK	
Formatowanie czasu, daty i wartości finansowych z polskim formatem	TAK	
Zapis wielu arkuszy kalkulacyjnych w jednym pliku.	TAK	
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..	TAK	
Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji	TAK	
Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:		
Przygotowywanie prezentacji multimedialnych, które będą: a) Prezentowanie przy użyciu projektora multimedialnego b) Drukowanie w formacie umożliwiającym robienie notatek c) Zapisanie jako prezentacja tylko do odczytu.	TAK	
Nagrywanie narracji i dołączanie jej do prezentacji	TAK	
Opatrywanie slajdów notatkami dla prezentera	TAK	
Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo	TAK	
Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego	TAK	
Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym	TAK	
Możliwość tworzenia animacji obiektów i całych slajdów	TAK	
Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera	TAK	
Pełna zgodność z formatami plików utworzonych za pomocą	TAK	

oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.		
Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:		
Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego	TAK	
Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców	TAK	
Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną	TAK	
Automatyczne grupowanie poczty o tym samym tytule	TAK	
Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy	TAK	
Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia	TAK	
Zarządzanie kalendarzem	TAK	
Udostępnianie kalendarza innym użytkownikom	TAK	
Przeglądanie kalendarza innych użytkowników	TAK	
Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach	TAK	
Zarządzanie listą zadań	TAK	
Zlecanie zadań innym użytkownikom	TAK	
Zarządzanie listą kontaktów	TAK	
Udostępnianie listy kontaktów innym użytkownikom	TAK	
Przeglądanie listy kontaktów innych użytkowników	TAK	
Możliwość przesyłania kontaktów innym użytkowników.	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy

22. Szczegółowa specyfikacja techniczna proponowanego oprogramowania antywirusowego – 187 sztuk – parametry muszą być zgodne z poniższymi tabelami oraz Zał. nr1 do SIWZ - SZCZEGÓŁOWE ZAŁOŻENIA TECHNICZNE PROJEKTU INFORMATYCZNEGO.

Oprogramowanie antywirusowe	**Wymagane minimalne parametry**	**Oferowane**
Producent, numer produktu, kraj pochodzenia (podać)		
Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/Windows 8/Windows 8.1.		
Wsparcie dla Windows Security Center (Windows XP SP2).	TAK	
Wsparcie dla 32- i 64-bitowej wersji systemu Windows.	TAK	
Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.	TAK	
Pomoc w programie (help) i dokumentacja do programu w języku polskim.	TAK	
Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark.	TAK	
Wsparcie dla: Windows Server 2008	TAK	
Ochrona antywirusowa i antyspyware		
Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.	TAK	
Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	TAK	
Wbudowana technologia do ochrony przed rootkitami.	TAK	
Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	TAK	
Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	TAK	
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.	TAK	
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 (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).	TAK	
Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.	TAK	
Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.	TAK	
Możliwość skanowania dysków sieciowych i dysków przenośnych.	TAK	
Skanowanie plików spakowanych i skompresowanych.	TAK	
Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).	TAK	

Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.	TAK	
Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.	TAK	
Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.	TAK	
Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.	TAK	
W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.	TAK	
Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.	TAK	
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.	TAK	
Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).	TAK	
Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail.	TAK	
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).	TAK	
Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.	TAK	
Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.	TAK	
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	TAK	
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.	TAK	
Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.	TAK	
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	TAK	

Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.	TAK	
Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK	
Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	TAK	
Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.	TAK	
Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	TAK	
Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.	TAK	
Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.	TAK	
W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.	TAK	
Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.	TAK	
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.	TAK	
Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).	TAK	
Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail.	TAK	
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).	TAK	
Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.	TAK	
Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.	TAK	
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	TAK	
Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa	TAK	

administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.		
Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.	TAK	
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.	TAK	
Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK	
Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	TAK	
Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.	TAK	
Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	TAK	
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	TAK	
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.	TAK	
Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.	TAK	
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.	TAK	
Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK	
Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	TAK	
Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.	TAK	
Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	TAK	
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	TAK	
Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa	TAK	

administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.		
Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.	TAK	
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.	TAK	
Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK	
Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	TAK	
Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.	TAK	
Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	TAK	
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	TAK	
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.	TAK	
Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.	TAK	
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.	TAK	
Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK	
Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	TAK	
Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.	TAK	
Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	TAK	
Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	TAK	
Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa	TAK	

administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.		
Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.	TAK	
Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	TAK	
Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.	TAK	
Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK	
Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.	TAK	
Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.	TAK	
Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.	TAK	
Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.	TAK	
W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.	TAK	
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.	TAK	
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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.	TAK	
Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.	TAK	
Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.	TAK	
Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.	TAK	

Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.	TAK	
Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.	TAK	
Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.	TAK	
Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.	TAK	
Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.	TAK	
Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie samo.	TAK	
Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.	TAK	
Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.	TAK	
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.	TAK	
System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.	TAK	
System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.	TAK	
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 oraz urządzeń przenośnych	TAK	
Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.	TAK	
Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.	TAK	
Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.	TAK	

W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.	TAK	
Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika	TAK	
Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).	TAK	
Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów: • tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.	TAK	
Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.	TAK	
Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.	TAK	
Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.	TAK	
Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.	TAK	
Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.	TAK	
Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.	TAK	
Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.	TAK	
Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.	TAK	
Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http	TAK	

Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).	TAK	
Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).	TAK	
Aplikacja musi być w pełni zgodna z technologią Network Access Protection (NAP).	TAK	
Program ma być w pełni zgodny z technologią CISCO Network Access Control (NAC).	TAK	
Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.	TAK	
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.	TAK	
Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.	TAK	
Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.	TAK	
Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.	TAK	
System zarządzania		
Centralna instalacja programów służących do ochrony stacji roboczych Windows.	TAK	
Centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows/ Linux/ MAC OS.	TAK	
Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi typu 2000/XP Professional/Vista/Windows7/Windows8.	TAK	
Do instalacji centralnej i zarządzania centralnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy	TAK	
Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem.	TAK	
Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.	TAK	
Kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup.	TAK	
Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.	TAK	
Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu	TAK	

ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).		
Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.	TAK	
Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.	TAK	
Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.	TAK	
Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.	TAK	
Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.	TAK	
Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).	TAK	
Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows 2000/XP/Vista/Windows 7/Windows 8 oraz na serwerach 2000/2003/2008/2008R2/2012 – 32 i 64-bitowe systemy.	TAK	
Możliwość rozdzielenia serwera centralnej administracji od konsoli zarządzającej, w taki sposób, że serwer centralnej administracji jest instalowany na jednym serwerze/ stacji a konsola zarządzająca na tym samym serwerze i na stacjach roboczych należących do administratorów.	TAK	
Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.	TAK	
Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.	TAK	
Serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.	TAK	
Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.	TAK	
Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.	TAK	
Aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres email.	TAK	

Do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji gdzie jest uruchomiona usługa serwera.	TAK	
Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).	TAK	
Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.	TAK	
Serwer centralnej administracji ma umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja ma otrzymać odpowiednią konfigurację.	TAK	
Serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę, oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.	TAK	
Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer ma informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych.	TAK	
W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną musi zostać poinformowany o tym fakcie za pomocą okna informacyjnego.	TAK	
Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.	TAK	
Aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem szyfrowanej komunikacji (za pomocą protokołu https).	TAK	
Do celu aktualizacji za pośrednictwem protokołu https nie jest wymagane instalowanie dodatkowych zewnętrznych usług jak IIS lub Apache zarówno od strony serwera aktualizacji jak i klienta.	TAK	
Dostęp do kwarantanny klienta ma być z poziomu systemu	TAK	

centralnego zarządzania.		
Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej administracji.	TAK	
Administrator ma mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej.	TAK	
Podczas przywracania pliku, administrator ma mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.	TAK	
Możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera centralnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.	TAK	
Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi.	TAK	
Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.	TAK	
Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu).	TAK	
W przypadku tworzenia administratora z niestandardowymi uprawnieniami możliwość wyboru modułów, do których ma mieć uprawnienia: zarządzanie grupami, powiadomieniami, politykami, licencjami oraz usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanna na klientach.	TAK	
Możliwość synchronizowania użytkowników z Active Directory w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania.	TAK	
Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane.	TAK	
Możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej.	TAK	
Panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne.	TAK	
Administrator musi posiadać możliwość tworzenia wielu	TAK	

zakładek, w których będą widoczne wybrane przez administratora elementy monitorujące.		
Elementy monitorujące muszą umożliwiać podgląd w postaci graficznej co najmniej: bieżącego obciążenia serwera zarządzającego, statusu serwera zarządzającego, obciążenia bazy danych z której korzysta serwer zarządzający, obciążenia komputera, na którym zainstalowana jest usługa serwera zarządzającego, informacji odnośnie komputerów z zainstalowaną aplikacja antywirusową, a które nie są centralnie zarządzane, podsumowania modułu antyspamowego, informacji o klientach znajdujących się w poszczególnych grupach, informacji o klientach z największą ilością zablokowanych stron internetowych, klientach, na których zostały zablokowane urządzenia zewnętrzne, informacje na temat greylistingu, podsumowania wykorzystywanych systemach operacyjnych, informacje odnośnie spamu sms, zagrożeń oraz ataków sieciowych	TAK	
Administrator musi posiadać możliwość maksymalizacji wybranego elementu monitorującego.	TAK	
Możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem.	TAK	
Możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback).	TAK	
Aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności.	TAK	
Wsparcie dla protokołu IPv6	TAK	
Administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej.	TAK	
Centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacji roboczej.	TAK	
Aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu.	TAK	
Aplikacja do administracji centralnej musi umożliwiać utworzenie nośnika, za pomocą którego będzie istniała możliwość przeskanowania dowolnego komputera objętego licencją przed startem systemu.	TAK	
Administrator musi posiadać możliwość określenia ilości jednoczesnych wątków instalacji centralnej oprogramowania klienckiego.	TAK	

1. Sposób wypełnienia tabeli podany jest w nawiasach przy nazwie wierszy.
2. Pozycja „podać” oznacz wartość zaproponowaną przez Wykonawcę.
3. Jeżeli podane wartości nie będą spełniać minimalnych wymaganych parametrów Oferta zostanie odrzucona.

.....

Podpis upełnomocnionego przedstawiciela Wykonawcy