Znak sprawy WOIT.271.25.2018

DRUK WZP-05

URZĄD MIASTA ZGIERZA
WYDZIAŁ ORGANIZACYJNY
Stanowisko ds. Informatyki i Telekomunikacji
95-100 Zgierz, Plac Jana Pawła II 16
tel. 42 714 31 59, fax 42 714 31 55
(pieczęć wydziału zamawiającego)

Załącznik nr 26.1.a
do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. NAZWA (I MIEJSCE) ZAMÓWIENIA:

Dostawa sprzętu komputerowego i oprogramowania w ramach projektu pn.:

"Wdrożenie i rozbudowa technologii informacyjno-komunikacyjnych w Gminie Miasto Zgierz", w ramach podziałania VII.1.2 technologie informacyjno-komunikacyjne Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020 współfinansowanego ze środków Europejskiego Funduszu Rozwoju.

2. KOD ZAMÓWIENIA[1]: GŁÓWNY PRZEDMIOT - 30232100-5
DODATKOWE PRZEDMIOTY - 48821000-9
32420000-3

3. OPIS PRZEDMIOTU ZAMÓWIENIA[1]:

Przedmiotem zamówienia jest dostawa, montaż i uruchomienie sprzętu teleinformatycznego i oprogramowania w Urzędzie Miasta Zgierza.

Część I.

Do Urzędu Miasta Zgierza należy dostarczyć, zamontować i uruchomić następujący sprzęt teleinformatyczny według opisu przedmiotu zamówienia:

- Serwer rakowy – 2 szt. (dostawa, instalacja, konfiguracja)
- Zasób taśmowy – 1 szt. (dostawa, instalacja, konfiguracja)
- Przełączniki sieciowe (z modułami STACK) – 2 szt. [dostawa, instalacja, konfiguracja]
- Router – 1 szt. (dostawa, instalacja, konfiguracja)
- Firewall – 1 szt. (dostawa, instalacja, konfiguracja)
- Komputery All-In-One – 50 szt. (dostawa)
- Komputery All-In-One – 10 szt. (dostawa)
- Pakiet biurowy – 60 szt. (dostawa)
- System operacyjny dla komputerów 60 szt. (dostawa, instalacja na komputerach zaoferowanych przez Wykonawcę – może być preinstalowany przez Producenta)
- System operacyjny serwerowy (rozbudowany) – 2 szt. [dostawa, instalacja na serwerach zaoferowanych przez Wykonawcę – może być preinstalowany przez Producenta]
- System operacyjny serwerowy (podstawowy) – 4 szt. [dostawa]
- Oprogramowanie antywirusowe (licencja na 300 stanowisk) [dostawa]
- Oprogramowanie do kopii bezpieczeństwa (dostawa, instalacja, konfiguracja)

Cały dostarczony sprzęt oraz oprogramowanie muszą być kompatybilne z rozwiązaniami technicznymi wdrożonymi u Zamawiającego w oparciu o następujący sprzęt i oprogramowanie:
CISCO FIREWALL ASA 5520
CISCO Switch 3750
CISCO Switch 3560G
CISCO Switch 2960-X
SERWER DELL R530
SERWER DELL R520
MACIERZ DYSKOWA DELL MD3800i
Domena MS Acitve Directory
SZAFA SERWEROWA Dell Netshelter SX 42U.

Zaoferowane oprogramowanie musi być: nowe, nieaktywowane nigdy wcześniej na innego użytkownika, pochodzące z oficjalnego kanału, jeżeli oprogramowanie nie pochodzi z polskiego rynku musi być objęte wymaganą przez Zamawiającego gwarancją świadczoną w Polsce. Oprogramowanie musi być dopuszczone do obrotu na terenie Unii Europejskiej. Zmawiający przeprowadzi procedurę sprawdzenia i weryfikacji legalności oprogramowania.

Zaoferowany sprzęt musi być: fabrycznie nowy (nieodnowiony). Pochodzący z oficjalnego kanału sprzedaży, jeżeli sprzęt nie pochodzi z polskiego rynku musi być objęty wymaganą przez Zamawiającego gwarancją świadczoną w Polsce. Sprzęt musi być dopuszczony do obrotu na terenie Unii Europejskiej. Zmawiający przeprowadzi procedurę sprawdzenia i weryfikacji legalności sprzętu i oprogramowania (wgranego/zainstalowanego na sprzęcie).

1. Serwer rakowy – 2 szt.
WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Obudowa	• Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). • Szyny montażowe musza być kompatybilne z szafą serwerową Zamawiającego Dell Netshelter SX 42U.
2.	Procesor	Min. dwa procesory dziesięciordzeniowe, x86 - 64 bity, Intel E5-2630v4 lub równoważne osiągające w testach SPECint_rate2006 wynik nie gorszy niż 830 punktów w konfiguracji dwuprocesorowej oferowanego modelu serwera lub w testach SPECint_rate2017 wynik nie gorszy niż 90 punktów w konfiguracji dwuprocesorowej oferowanego modelu serwera. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
3.	Płyta główna	Obsługująca min. 2 procesory.
4.	Pamięć operacyjna	• Min. 128 GB RDIMM DDR4 w modułach o pojemności min 32GB każdy. • Płyta główna musi posiadać min. 24 sloty na pamięć i umożliwiać rozbudowę do minimum 3TB LRDIMM lub 768GB RDIMM lub min. 128GB NVDIMM (dowolny rodzaj).

		• Obsługa zabezpieczeń min: Advanced ECC i Online Spare.
5.	Sloty rozszerzeń	Serwer musi posiadać minimum 4 sloty PCI-Express w tym: • Minimum 3 sloty PCI-Express Generacji 3 działające z prędkością x8 (bus width). • Minimum 1 slot PCI-Express Generacji 3 działający z prędkością x16 (bus width) pełnej długości i wysokości.
6.	Dysk twardy	Zainstalowane dyski: • Min. 2x400GB SSD 6Gb/s. • Min. 4x 2TB SAS 10k 12Gb/s. Możliwość zainstalowania min. 16 dysków typu Hot Swap, SAS/SATA/SSD, 2,5". Obudowa serwera musi umożliwiać rozbudowę/rekonfigurację do obsługi min. 26 wewnętrznych dysków SFF SAS/SATA/SSD, 2,5". Rekonfiguracja powyżej 16 dysków może być możliwa poprzez zastąpienie innych elementów wyposażenia np. DVD slotami na dyski.
7.	Kontroler	• Kontroler macierzowy SAS min. 12Gb z min. 2GB cache, z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę do min. 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID min. 0/1/1+0/5/5+0/6/6+0. • Możliwość rozbudowy pamięci cache do min. 4GB poprzez rozbudowę kontrolera lub wymianę kontrolera.
8.	Interfejsy sieciowe	• Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45, które nie zajmują gniazd PCIe. • Min. wbudowane lub zainstalowane 2 porty obsługujące prędkości 10Gb BaseT lub SFP+. W przypadku zastosowania dodatkowych elementów ww., muszą być one dostarczone przez Wykonawcę i kompatybilne z zaoferowanymi przełącznikami z punktu 3. "Przełączniki sieciowe". Min. 2 szt. kabel sieciowy o długości min 7m. Komunikacja z przełącznikami musi odbywać się z prędkością, którą oferują porty 10GE. Gwarancja min. 1 rok dla modułu/wkładek/okablowania.
9.	Karta graficzna	Zintegrowana karta graficzna.
10.	Porty	• 5 x USB 3.0 (dopuszcza się zastosowanie zewnętrznego kontrolera USB 3.0 zainstalowanego w slocie PCI-Express). • 1x VGA. • Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy o min: • Dodatkowy port VGA dostępny z przodu serwera. • Port szeregowy. Nie dopuszczalne jest stosowanie przejściówek ani kart PCI w celu uzyskania wymaganej powyżej funkcjonalności micro SD, VGA.
11.	Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
12.	Chłodzenie	• Zestaw wentylatorów redundantnych typu hot-plug. • Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4.
13.	Napęd	DVD-RW.
14.	Karta/Moduł zarządzający/Dodatkowe oprogramowanie	• Moduł zdalnego zarządzania (konsoli) pozwalającej na min.: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS).

		• Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. • Moduł zdalnego zarządzania musi posiadać wbudowaną pamięć flash, minimum 4GB, w tym minimum 1GB dostępny dla użytkownika serwera. Moduł zarządzania zdalnego, musi udostępniać wbudowane narzędzie wspomagające instalację systemów operacyjnych oraz konfigurację serwera. Narzędzie dostępne z poziomu BIOS poprzez interfejs graficzny (GUI), udostępniające minimum następujące funkcjonalności: • Wspomaganą instalację systemu operacyjnego – wybór najlepszych sterowników i firmware. • Diagnostykę wszystkich elementów sprzętowych serwera. • Konfigurację kontrolera macierzowego i dysków poprzez GUI. • Ustawienia parametrów BIOS. Rozwiązanie sprzętowe (tzn. Moduł), niezależne od systemów operacyjnych, zintegrowane z płytą główną lub montowane niezależnie na płycie głównej, nieograniczające w żaden sposób dostępnych wymaganych portów/slotów w zaoferowanym Serwerze, posiadające dedykowany port RJ45. Wymagana odpowiednia licencja spełniająca w/w parametry.
15.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	• Microsoft Windows Server. • Red Hat Enterprise Linux (RHEL). • SUSE Linux Enterprise Server (SLES). • Canonical Ubuntu. • Oracle Linux. • CentOS. • Vmware. • Citrix XenServer.
16.	Wsparcie techniczne/Gwarancja	• Min. 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. • W przypadku awarii dyski twarde pozostają własnością zamawiającego.
17.	Inne	• Urządzenia muszą być fabrycznie nowe, zakupione w oficjalnym kanale dystrybucyjnym producenta. • Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. • Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. • Deklaracja zgodności CE.
18.	Instalacja i konfiguracja	• Instalacja dostarczonego serwera we wskazanej przez Zamawiającego szafie rack Dell Netshelter SX 42U. • Instalacja systemu operacyjnego (system również może być preinstalowany przez Producenta). • Instalacja RAID na dyskach: RAID-1 i RAID-10. • Zainstalowanie/konfiguracja dostarczonego oprogramowania wirtualizacyjnego na serwerze. • Konfiguracja klastra w oparciu o dostarczone serwery przez Wykonawcę przy użyciu oprogramowania z Pozycji 10 "System operacyjny serwerowy". • Migracja maszyn wirtualnych z istniejących serwerów wirtualizacyjnych na uruchomiony klaster.

		• Przeprowadzenie testów awaryjnych wdrożonego środowiska – klastra (symulacja awarii pojedynczego węzła klastra). • Instalacja dostarczonych modułów SFP+ (w razie konieczności).

2. Zasób taśmowy – 1 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Obudowa	• Oferowana biblioteka musi być przystosowana do montażu w szafie 19". • Wysokość oferowanej biblioteki taśmowej nie może przekraczać 2U. • Szyny montażowe muszą być kompatybilne z szafą serwerową Zamawiającego Dell Netshelter SX 42U.
2.	Napęd/Parametry	Biblioteka taśmowa musi być wyposażona w min. 1 napęd LTO-6 SAS oraz musi umożliwiać zastosowanie taśm, co najmniej 2,5TB każda – parametry podane bez kompresji danych.
3.	Sloty	• Oferowana biblioteka musi być wyposażona, w co najmniej 24 sloty na taśmy magnetyczne. • Jeżeli licencjonowana jest liczba slotów - wymagane jest aktywowanie wszystkich slotów przez Wykonawcę.
4.	Zarządzanie	Oferowana biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej oraz musi mieć możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD.
5.	Czytnik	Oferowana biblioteka taśmowa musi być wyposażona w czytnik kodów kreskowych.
6.	Taśmy	Wraz z biblioteką należy dostarczyć min. 20 szt. taśm LTO-6 RW min. 2,5TB (bez kompresji) wraz z etykietami oraz min. 1 szt. taśmę czyszczącą.
7.	Funkcjonalność	• Oferowany napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu. • Obsługa min. SAS 6Gb.
8.	MTBF	Dla oferowanej biblioteki parametr MTBF musi wynosić, co najmniej 100 000 godzin.
9.	MSBF	Dla oferowanej biblioteki parametr MSBF musi wynosić, co najmniej 1 000 000 pełnych cykli „załaduj/wyładuj".
10.	Szyfrowanie	• Biblioteka musi posiadać wsparcie dla technologii szyfrowania backupowanych danych. • Oferowana biblioteka musi posiadać port USB przeznaczony do współpracy ze sprzętowym kluczem USB w celu przechowywania kluczy szyfrujących, w innym przypadku musi być dostarczona z dedykowany serwer oraz oprogramowanie do przechowywania kluczy.
11.	Gwarancja	Min. 3 lata z gwarantowanym czasem NBD od momentu odebrania zgłoszenia przez serwis. Uszkodzony nośnik danych po wymianie musi pozostać u użytkownika. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego sprzętu.
12.	Konfiguracja	• Instalacja dostarczonego Zasobu taśmowego we wskazanej przez Zamawiającego szafie rack Dell Netshelter SX 42U. • Instalacja taśm w napędzie/slotach. • Instalacja/podłaczenie zasobu taśmowego na serwerze Dell R530

		Service Tag:D8Z9QK2.
13.	Normy	Biblioteka musi posiadać wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja).
14.	Elementy dodatkowe/montażowe	• Dodatkowy moduł/kontroler SAS min. 6Gb do serwera Dell R530 Service Tag: D8Z9QK2 wraz z okablowaniem o długości min. 1m w celu podłączenia zasobu taśmowego (SAS) dostarczony przez Wykonawcę. Gwarancja min 1 rok.

3. Przełączniki sieciowe (w tym moduły STACK) – 2 szt.
WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Typ/Opis	• Zarządzany przełącznik warstwy min. 2 ISO OSI. • Urządzenie musi mieć możliwość dodania do obecnie używanego stosu przez Zamawiającego opartego na przełącznikach Cisco 2960-X.
2.	Obudowa	• Urządzenie przystosowane jest do montażu w szafie stelażowej 19". • Wraz z urządzeniem dostarczone są niezbędne elementy do montażu w szafie stelażowej. • Wysokość urządzenia: maksymalnie 1U. • Urządzenie posiada, co najmniej następujące diody statusowe: działanie urządzenia, działanie wbudowanych portów Ethernet.
3.	Interfejsy	• Co najmniej 24 zabudowane w urządzeniu gniazda 10Base-T/100Base-TX/1000Base-T automatycznie rozpoznające kable proste / krzyżowe. • Zabudowany w urządzeniu port konsoli lokalnej w standardzie RS232 zakończony gniazdem RJ-45 lub inny (w przypadku innego portu konsoli niezbędne jest dostarczenie wymaganego okablowania/przejściówki). • Urządzenie posiada możliwość montażu, co najmniej dwóch interfejsów (modułów) w standardzie SFP+ 10 Gigabit Ethernet (Small Form-Factor Pluggable). Interfejsy muszą być kompatybilne z zaoferowanymi serwerami przez Wykonawcę. Zamawiający wymaga dostarczenia wkładek 10GE przez Wykonawcę. Gwarancja na wkładki min 1 rok. • Urządzenie musi posiadać możliwość pracy w stosie po zastosowaniu dedykowanego modułu wewnętrznego tworząc jedno urządzenie logiczne z minimum 8 urządzeniami fizycznymi • Przepustowość dedykowanego interfejsu na potrzeby stosu nie mniejsza niż 40Gbps.
4.	Pamięć wewnętrzna	• Minimum 128 MB pamięci flash. • Minimum 512 MB pamięcie DRAM.
5.	Protokoły i standardy	• Statyczny routing IPv4. • Wsparcie min. protokołów sieciowych: NTP, SSH , SSH-2, serwera/klienta DHCP filtrowanie adresów MAC, SNMPv1/2/3, SCP, TACACS+, RADIUS Serwer/Klient, BPDU Guard, SPAN, Telnet, VTPv3, EtherChannel, Voice VLAN, Guest VLAN , STP/RSTP, IPv4 Port-Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, MAC Authentication Bypass, 802.1x MultiDomain Authentication, Storm Control, Trust Boundary, Access-List (ACL). • Pełna obsługa standardów min: IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z, IEEE 802.1, 802.3, IEEE 802.1q VLAN, IEEE

		802.1s Multiple Spanning-Trees, IEEE 802.1w Rapid Spanning-Tree, IEEE 802.1x Port Access Authentication, IEEE 802.1AB LLDP, IEEE 802.3ad Link Aggregation (LACP). • Urządzenie musi być kompatybilne z protokołem NetFlow v9, JFlow lub odpowiednikiem.
6.	Wydajność przełączania	• Przepustowość przełączania minimum 215 Gbps. • Przepustowość przekazywania minimum 107 Gbps.
7.	Usługi przełączania	• Urządzenie musi obsługiwać minimum 4096 identyfikatorów sieci VLAN, przy czym co najmniej 1023 z nich są aktywne. • Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów. • Urządzenie musi obsługiwać minimum 16000 adresów MAC. • Urządzenie poprawnie obsługuje protokoły IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree.
8.	Zasilanie	• Urządzenie zasilane z napięcia zmiennego 230V / 50Hz. • Urządzenie dostarczane wraz ze standardowym kablem zasilającym o długości co najmniej 1,5m z wtykiem CEE7/7.
9.	Zarządzanie	• Urządzenie może synchronizować wewnętrzny czas przy użyciu protokołu NTP. • Urządzenie można konfigurować przy użyciu linii komend oraz dedykowanej aplikacji. • Urządzenie można konfigurować zdalnie przy użyciu protokołów TELNET, SSH oraz dedykowanej aplikacji. - Urządzenie może korzystać z wewnętrznej i zewnętrznej bazy użytkowników (RADIUS). • Urządzenie umożliwia uwierzytelnianie użytkowników. • Każdemu z użytkowników można przypisać poziom uprawnień, do którego jednoznacznie przypisane są określone polecenia urządzenia • Urządzenie umożliwia konfigurację przy użyciu tekstowych plików konfiguracyjnych możliwych do edytowania poza urządzeniem. • Urządzenie umożliwia wysyłanie wybranych wiadomości, co najmniej do wewnętrznego bufora logów, na konsolę lokalną, konsolę konfiguracji zdalnej (Telnet, SSH) oraz na zewnętrzny serwer Syslog. • Urządzenie jest kompatybilne z protokołem SNMP w wersji 1, 2 i 3. • Urządzenie do konfiguracji musi wykorzystywać listy kontroli dostępu (ACL) lub inny mechanizm o podobnym działaniu. • Urządzenie wspiera protokół VTP.
10.	Niezawodność	Parametr MTBF minimum 564,000 godzin.
11.	Gwarancja i serwis	Gwarancja min. 5 lat, uprawniająca do zgłaszania usterek sprzętowych i oprogramowania, świadczona w reżimie 8x5xNBD, umożliwiająca pobieranie nowych wersji oprogramowania, dostęp do pomocy technicznej oraz bazy wiedzy i narzędzi zarządzających.
12.	Wkładki/Moduły	Moduł stackujący kompatybilny z przełącznikami Cisco 2960-X posiadanymi przez Zamawiającego oraz z przełącznikami oferowanymi przez Wykonawcę (wraz z kablem stackującym o długości min. 50 cm) – 1 sztuka. Gwarancja min. 1 rok.
13.	Instalacja/Konfiguracja	Dostarczone przełączniki musza zostać uformowane w stos z posiadanymi przez Zamawiającego przełącznikami Cisco 2960-X. Konfiguracja w zakresie m.in. VLAN, STP.

4. Router – 1 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Przepustowość	Min. 500 Mbps z możliwością podniesienia do min. 1Gbps (darmowo lub odpłatnie).
2.	Liczba portów	Min. 4 szt. GE Ethernet (wbudowane lub możliwe do uzyskania poprzez zastosowanie wkładek), w przypadku portów SFP, Wykonawca musi dostarczyć wymagane wkładki (GE). W przypadku zastosowania wkładek, gwarancja na wkładki min. 1 rok.
3.	Oprogramowanie/ Funkcjonalność	• Musi obsługiwać min. BGPv4 (w tym 4 bitowe SN), OSPFv3, RIPv2, ISIS, routing statyczny, NTP, 802.1q, DHCP (w zakresie klient, Serwer), ICMP, WCCP, WCCPv2, WRED, HSRP (lub odpowiednik), MPLS, uRPF, BFD (lub odpowiednik). • Musi zapewniać obsługę list kontroli dostępu w oparciu o min. adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL. • Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3. • Funkcjonalność musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych. • Funkcjonalność musi pozwalać na generowanie akcji takich jak: wykonanie komendy z poziomu linii poleceń urządzenia, wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej, wykonanie skryptu, wygenerowanie SNMP trap, ustawienie lub modyfikacja określonego licznika systemowego.
4.	Sloty do rozszerzeń	Tak z możliwością/wsparciem obsadzenia min. kartami: • z przełączanymi portami GE (10/100/1000) z obsługą PoE+ (IEEE 802.3at). • z modemem 4G (LTE Advanced). • z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł oraz 8 portów per moduł.
5.	Porty USB	Min. 1 szt.
6.	IPSEC VPN	Tak.
7.	Zabezpieczenia	• Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów min. RADIUS. • Obudowa musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
8.	Pamięć DRAM	Min. 16 GB.
9.	Pamięć FLASH	Min. 8 GB.
10.	Wymiary	Max. 2U – 19 cali.
11.	Głośność pracy	Max. do 85 dBA (pod obciążeniem).
12.	Temperatura pracy	W zakresie min. 0 do 40^{0}C.

13.	Waga	Max. do 12 kg.
14.	Pobór prądu	Max. do 1000W.
15.	Zestaw montażowy	Odpowiedni dla standardowej uniwersalnej szafy 19 cali.
16.	Instalacja/Konfiguracja	Wykonawca musi skonfigurować urządzenie w oparciu o wytyczne od Zmawiającego min. (Routing statyczny, dynamiczny).
17.	Zarządzanie	• Zabudowany w urządzeniu port konsoli lokalnej w standardzie RS232 zakończony gniazdem RJ-45 lub inny (w przypadku innego portu konsoli niezbędne jest dostarczenie wymaganego okablowania/przejściówki). • Urządzenie musi być zarządzane za pomocą min. SNMPv1, SNMPv2, SNMPv3, Telnet, SSH. • Urządzenie musi mieć możliwość konfiguracji poprzez interfejs graficzny. • 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 dowolnej ilości plików konfiguracyjnych (ograniczenie może stanowić wbudowana pamięć urządzenia). Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
18.	Gwarancja	• Min. 5-letnia gwarancja uprawniająca do zgłaszania usterek sprzętowych i oprogramowania, świadczona w reżimie 8x5xNBD, umożliwiająca pobieranie nowych wersji oprogramowania, dostęp do pomocy technicznej oraz bazy wiedzy i narzędzi zarządzających.

5. Firewall – 1 szt.
WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Przepustowość	Min. 2 Gbps.
2.	Liczba VLAN	Min. 200.
3.	Jednoczesne połączenia	Min. 500 000.
4.	Dostępność	Mechanizmy redundancji min. aktywny/aktywny, aktywny/gotowość.
5.	Nowe połączenia	Min. 20 000 na sekundę.
6.	Porty USB	Min 2 szt. USB 2.0.
7.	Tunele	Min. 700 IPsec peers.
8.	Porty GE	Min 8 szt. Gigabit Ethernet.
9.	Możliwość rozbudowy portów	Tak (w celu dodania nowych portów GE Ethernet lub/i SFP) o min. 6 szt.
10	Funkcjonalność/ Oprogramowanie	Min. NAT, PAT, NTP, Routing (RIP, OSPF, BGP, STATIC), SSH, 802.1q, SNMP, ICMP,

		Urządzenie musi zapewniać funkcjonalność w zakresie nie mniejszym niż: • System automatycznego wykrywania klasyfikacji aplikacji (SWA) musi min: - umożliwiać tworzenie profili użytkowników z dokładnością, co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług, - umożliwiać współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez SWA oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach. • System IPS musi min.: - posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system, - posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu), - posiadać możliwość wykrywania i uniemożliwiać szeroką gamę zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługę VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.), - zapewniać, co najmniej poniższe sposoby wykrywania zagrożeń: ✓ sygnatury ataków opartych na exploitach, ✓ reguły oparte na zagrożeniach, mechanizm wykrywania, anomalii w protokołach, ✓ mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego. - zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS, - urządzenie musi zostać dostarczone wraz z licencjami umożliwiającymi działanie funkcjonalności IPS oraz systemu automatycznego wykrywania klasyfikacji aplikacji (w wypadku licencjonowania okresowego, dostarczone licencje powinny obejmować okres nie mniejszy niż gwarancja urządzenia). • Oferowane rozwiązanie zapory ogniowej musi być oparte o dedykowany system operacyjny. Nie dopuszcza się rozwiązań gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim posadowione oprogramowanie firewall (jako aplikacja). Ponadto musi umożliwiać pracę zapory ogniowej (ang. firewall) w trybie warstwy 3 (routed) i warstwy 2 (transparentnym). • Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników. Oferowane rozwiązanie musi zawierać oprogramowanie do centralnego zarządzania umożliwiające, co najmniej: • Zarządzanie urządzeniami, licencjami, zdarzeniami i politykami. • Kompleksowe raportowanie i ostrzeżenia dotyczące zarówno ogólnych, jak i ukierunkowanych informacji. • Monitoring zachowania i wydajności sieci. • Funkcje korelacji w zakresie reagowania na zagrożenia w czasie rzeczywistym. • Obsługę minimum 2 urządzeń oraz przechowywanie, co najmniej

		250GB danych zdarzeń. Oprogramowanie do centralnego zarządzania musi oferować otwarte API umożliwiające integrację rozwiązań firm trzecich oraz musi być dostarczone jako wirtualne urządzenie na hypervisor min. VMWare.
11.	Pamięć	Min. 8GB.
12.	Pamięć FLASH	Min. 8 GB.
13.	Wymiary	Max. 1U – 19 cali.
14.	Dodatkowa pamięć	Dysk min. 120GB (zainstalowany w urządzeniu, wymienny).
15.	Poziom głośności	Max. do 65 dBA.
16.	Waga	Max. do 15kg.
17.	Temperatura pracy	W zakresie min. 0 do 40^{0}C
18.	Pobór Energi elektrycznej	Max. do 200W.
19.	Zarządzanie	• Zabudowany w urządzeniu port konsoli lokalnej w standardzie RS232 zakończony gniazdem RJ-45 lub inny (w przypadku innego portu konsoli niezbędne jest dostarczenie wymaganego okablowania/przejściówki). • Konfiguracja poprzez interfejs graficzny. • Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.
20.	Logi	Zaoferowane urządzenie musi być kompatybilne z oprogramowaniem do zbierania/analizy logów posiadanym przez Zamawiającego ManageEngine Firewall Analyzer.
21.	Instalacja/Konfiguracja	Wykonawca musi skonfigurować urządzenie w oparciu o wytyczne od Zmawiającego min. (Routing statyczny, dynamiczny, NAT, tunele VPN, ACl, QOS). Konfiguracja w zakresie bezpieczeństwa i dobrych praktyk.
22.	Gwarancja	Min. 5-letnia gwarancja uprawniająca do zgłaszania usterek sprzętowych i oprogramowania, świadczona w reżimie 8x5xNBD, umożliwiająca pobieranie nowych wersji oprogramowania, aktualizację definicji oprogramowania zabezpieczającego (IPS, wykrywanie aplikacji), dostęp do pomocy technicznej oraz bazy wiedzy i narzędzi zarządzających.

6. Komputery All-In-One– 50 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Ekran	• Przekątna: min 21,5". • Rozdzielczość: min. FHD 1080p (1920x1080). • Matryca matowa lub błyszcząca z filtrem antyrefleksyjnym.
2.	Obudowa	• Zintegrowana z monitorem (AIO). • Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) lub kłódki (oczko w obudowie do założenia kłódki).
3.	Chipset	Dostosowany do zaoferowanego procesora.
4.	Płyta główna	• Dostosowana do zaoferowanego komputera.

		• Wyposażona w min. 2 złącza M.2, z czego jedno obsługujące dysk SSD PCIe NVMe.
5.	Procesor	Procesor klasy x86, min. 4 rdzeniowy, zaprojektowany do pracy w komputerach stacjonarnych, taktowany zegarem, co najmniej 2,4 GHz, pamięcią cache L3, co najmniej 6 MB lub równoważny wydajnościowo osiągający wynik co najmniej 6550 pkt w teście PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net.
6.	Pamięć operacyjna	• Min. 8 GB DDR4. • Ilość banków pamięci: min. 2 szt.
7.	Dysk twardy	Min. 500GB SATA lub min. 240GB SSD.
8.	Napęd optyczny	Nagrywarka DVD +/-RW.
9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu, dynamicznie przydzielaną na potrzeby grafiki w wielkości, co najmniej 1,5GB. Wsparcie min. DirectX 11 i OpenGL 4.0
10.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo, wbudowany mikrofon, wbudowana kamera min. HD720p z mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery.
11.	Karta sieciowa	• Min. 1 szt. LAN 10/100/1000 Mbit/s. • Min. 1 szt. WiFi 1x1 AC + min 1 szt. BT 4.
12.	Porty/złącza	Wbudowane: • Min. 1 szt. HDMI lub/i DisplayPort. Min. 6 szt. USB w tym min. 2 szt. USB 3.1. • Min. 1 szt. wyjście na słuchawki/wejście na mikrofon (combo) , czytnik kart pamięci min 4 w1. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
13.	Klawiatura/mysz	• Klawiatura przewodowa w układzie polski programisty. • Mysz przewodowa z rolką (scroll).
14.	Zasilacz	Maksymalna moc zasilacza dostosowana do zaoferowanego komputera.
15.	System operacyjny	• Preinstalowany na partycji do odzyskiwania systemu przez Producenta/Wykonawcę lub dostarczony na odpowiednim nośniku zewnętrznym np. USB, DVD. • Komputer musi być zgodny z systemem operacyjnym z punktu: 9 "System dla komputerów". • System operacyjny musi być zainstalowany na zaoferowanym komputerze przez Wykonawcę lub Producenta.
16.	BIOS	• BIOS zgodny ze specyfikacją UEFI. • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji min. o: - modelu komputera, producencie komputera, - numerze seryjnym, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, - ilości pamięci RAM wraz z taktowaniem, - napędach lub dyskach podłączonych do portów. 1. Możliwość min. z poziomu Bios: - wyłączenia selektywnego (pojedynczego) portów USB, - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia wbudowanej kamery, karty WiFi, karty audio, mikrofonu, czytnika kart, - ustawienia hasła: administratora, - wglądu w system zbierania logów z możliwością czyszczenia logów,

		- wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan), - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii, - załadowania optymalnych ustawień Bios.
17.	Zintegrowany System Diagnostyczny	• Wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami (działający nawet w przypadku uszkodzenia dysku twardego) w szczególności: • Wykonanie testu pamięci RAM. • Wykonanie testu dysku twardego. • Wykonanie testu CPU. • Wykonanie testu portów USB.
18.	Certyfikaty i standardy	• Certyfikat min. ISO 9001: 2000 dla producenta sprzętu. • ENERGY STAR. • Deklaracja zgodności CE. • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
19.	Waga/rozmiary urządzenia	• Waga urządzenia wraz ze stopą max. 20kg.
20.	Gwarancja	• Min. 2 lata świadczona w miejscu użytkowania sprzętu (on-site). • Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. • W przypadku awarii dyski twarde pozostają własnością zamawiającego. • Firma serwisująca musi posiadać min. ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta sprzętu.
21.	Wsparcie techniczne producenta	• Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. • Możliwość weryfikacji konfiguracji fabrycznej zakupionego sprzętu. • Możliwość weryfikacji posiadanej/wykupionej gwarancji. • Możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego.

7. Komputery All-In-One– 10 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Ekran	Przekątna: min 23 cale. Rozdzielczość: min. FHD 1080p (1920x1080), matryca matowa lub błyszcząca z filtrem antyrefleksyjnym.
2.	Obudowa	Zintegrowana z monitorem (AIO).
3.	Chipset	Dostosowany do zaoferowanego procesora.
4.	Płyta główna	Dostosowana do zaoferowanego komputera.
5.	Procesor	Procesor wielordzeniowy (min. 4 rdzenie), ze zintegrowanym układem graficznym, dedykowany do pracy w komputerach stacjonarnych, osiągający w teście PassMark CPU Mark wynik min. 8000 pkt. Układ musi pracować z fabrycznymi ustawieniami producenta

		(niedozwolony tzw. „overclocking"). Wynik procesora weryfikowany wyłącznie na podstawie listy wyników testów, opublikowanej na stronie www.cpubenchmark.net.
6.	Pamięć operacyjna	Min. 16GB.
7.	Dysk twardy	Min. 240GB SSD.
8.	Napęd optyczny	Nagrywarka DVD +/-RW.
9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu, dynamicznie przydzielaną na potrzeby grafiki w wielkości, co najmniej 1,5GB. Wsparcie min. DirectX 11 i OpenGL 4.0. **Dedykowana karta graficzna z własna pamięcią min. 2GB. Wsparcie min. DirectX 11 i OpenGL 4.0.**
10.	Audio	Karta dźwiękowa zgodna z High Definition.
11.	Karta sieciowa	• Min. 1 szt. LAN Min. • Min. 1 szt. WiFi.
12.	Porty/złącza	Wbudowane: • Min. 1 szt. HDMI lub/i DisplayPort. • Min. 8 szt. USB w tym min. 2 szt. USB 3.0. • Min. 1 x wyjście na słuchawki. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
13.	Klawiatura/mysz	• Klawiatura w układzie polski programisty. • Mysz z rolką (scroll).
14.	Zasilacz	Maksymalna moc zasilacza nie większa niż 200W.
15.	System operacyjny	Preinstalowany na partycji do odzyskiwania systemu przez Producenta/Wykonawcę lub dostarczony na odpowiednim nośniku zewnętrznym np. USB, DVD. Komputer musi być zgodny z systemem operacyjnym z pozycji: 9 "System dla komputerów".
16.	Bios	• BIOS zgodny ze specyfikacją UEFI • Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych, uzyskania informacji, co najmniej o: - modelu komputera, - numerze seryjnym, - MAC Adres karty sieciowej, - zainstalowanym procesorze, - ilości pamięci RAM, - podłączonych dyskach do portów SATA (model dysku twardego).
17.	Zintegrowany System Diagnostyczny	Wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami (działający nawet w przypadku uszkodzenia dysku twardego) w szczególności: • Wykonanie testu pamięci RAM. • Wykonanie testu dysku twardego.
18.	Certyfikaty i standardy	• Certyfikat min. ISO 9001:2000 dla producenta sprzętu. • ENERGY STAR. • Deklaracja zgodności CE. • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
19.	Waga/rozmiary urządzenia	Waga urządzenia wraz ze stopą max. 20kg.

20.	Gwarancja	• Min. 2 lata świadczona w miejscu użytkowania sprzętu (on-site). • W przypadku awarii dyski twarde pozostają własnością zamawiającego. • Firma serwisująca musi posiadać min. ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta sprzętu. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta.

8. Pakiet biurowy– 60 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Pakiet biurowy	**Pakiet biurowy z interfejsem i słownikiem w języku polskim** Microsoft Office 2016 H&B- licencja wieczysta (z nośnikiem i/lub licencją elektroniczną) fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika lub **równoważny*.** ***Zamawiający przez równoważność rozumie:** Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.: • Edytor tekstów. • Arkusz kalkulacyjny. • Narzędzie do przygotowania i prowadzenia prezentacji. • Narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). • Pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. • Powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. • Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-16 – cena połączenia nie większa niż cena połączenia lokalnego. • Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa, co najmniej 5 lat od daty zakupu. • Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). **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. • Wstawianie oraz formatowanie tabel. • Wstawianie oraz formatowanie obiektów graficznych. • Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). • Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.

		• Automatyczne tworzenie spisów treści. • Formatowanie nagłówków i stopek stron. • Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. • Określenie układu strony (pionowa/pozioma). • Wydruk dokumentów. • Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. **Arkusz kalkulacyjny musi umożliwiać:** • Tworzenie raportów tabelarycznych. • Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. • Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. • Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). • Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. • Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. • Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. • Wyszukiwanie i zamianę danych. • Wykonywanie analiz danych przy użyciu formatowania warunkowego. • Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. • Formatowanie czasu, daty i wartości finansowych z polskim formatem. • Zapis wielu arkuszy kalkulacyjnych w jednym pliku. • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. **Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:** • Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego. • Drukowanie w formacie umożliwiającym robienie notatek. • Zapisanie, jako prezentacja tylko do odczytu. • Nagrywanie narracji i dołączanie jej do prezentacji. • Opatrywanie slajdów notatkami dla prezentera. • Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.

		• Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. • Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. • Możliwość tworzenia animacji obiektów i całych slajdów. • Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. **Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:** • Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. • Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. • Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. • Automatyczne grupowanie poczty o tym samym tytule. • Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. • Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. • Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. • Zarządzanie kalendarzem. • Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. • Przeglądanie kalendarza innych użytkowników. • Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. • Zarządzanie listą zadań. • Zlecanie zadań innym użytkownikom. • Zarządzanie listą kontaktów. • Udostępnianie listy kontaktów innym użytkownikom. • Przeglądanie listy kontaktów innych użytkowników. • Możliwość przesyłania kontaktów innym.

9. System operacyjny dla komputerów– 60 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	System operacyjny	**System musi być zainstalowany na komputerach z punktu 6 i 7.** System operacyjny Windows 10 Professional 64-bit w języku polskim, fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika lub równoważny*. ***Zamawiający przez równoważność rozumie (min. parametry):** System operacyjny klasy desktop musi spełniać następujące min. wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych

		aplikacji: • Interfejs graficzny użytkownika pozwalający na obsługę: - klasyczną przy pomocy klawiatury i myszy, - dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, • Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe. • Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje. • Wbudowany system pomocy w języku polskim. • Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. • Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. • Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. • Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne. • Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. • Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. • Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących, lub ograniczających funkcjonalność systemu lub aplikacji, • Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.

		• Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Obsługa standardu NFC (near field communication). • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. • Mechanizmy uwierzytelniania w oparciu o: - login i hasło, - karty z certyfikatami (smartcard), - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), - wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO. • Mechanizmy wieloskładnikowego uwierzytelniania. • Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. • Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. • Wsparcie dla algorytmów Suite B (RFC 4869). • Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji. • Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku. • Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym. • Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny. • Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0. • Możliwość selektywnego usuwania konfiguracji oraz danych określonych, jako dane organizacji. • Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu. • Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. • Wbudowane narzędzia służące do administracji, do wykonywania

		kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. • Wsparcie dla środowisk Java i NET Framework 4.X – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. • Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning). • Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. • Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. • Udostępnianie wbudowanego modemu. • Oprogramowanie dla tworzenia kopii zapasowych (Backup) - automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. • Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). • Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. • Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. • Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. • Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. • Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. • Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

10. System operacyjny serwerowy (rozbudowany) – 2 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	System operacyjny	Windows Server Data Center Core 2016 MOLP GOV– fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika z nośnikiem i/lub licencją elektroniczną, wraz z serwerem należy dostarczyć wymaganą ilość licencji (20 rdzeni), zainstalowany na dostarczonych serwerach przez Wykonawcę/Producenta z przeprowadzoną konfiguracją klastra – lub równoważny*. System na nośniku danych ***Przez równoważność zamawiający rozumie (min. parametry):** • Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. • 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. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy, jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: - pozwalają na zmianę rozmiaru w czasie pracy systemu, - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, - umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

		• Dostępne dwa rodzaje graficznego interfejsu użytkownika: - klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, - dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. • Mechanizmy logowania w oparciu o: - login i hasło, - karty z certyfikatami (smartcard), - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). • Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). • Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: - podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, - 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: ✓ podłączenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną, ✓ ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania, ✓ odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, ✓ bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows. - Zdalna dystrybucja oprogramowania na stacje robocze. - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

		✓ dystrybucję certyfikatów poprzez http, ✓ konsolidację CA dla wielu lasów domeny, ✓ automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, ✓ automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. - szyfrowanie plików i folderów, - szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), - możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, - Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersjach 4 oraz 6 (IPv4; IPv6). Wsparcie dla algorytmów Suitę B (RFC 4869). • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - obsługi ramek typu jumbo frames dla maszyn wirtualnych, - obsługi 4-KB sektorów dysków, - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, - 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 serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. • Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. **System musi współpracować z posiadanymi i wdrożonymi przez Zamawiającego w pełni usługami: min. Active Directory, DNS, DHCP. Zamawiający posiada wymagane licencje dostępowe MS CAL 2016.**

		System musi być zainstalowany na serwerach zaoferowanych z punktu 1. "1. Serwer rakowy – 2 szt.".

11. System operacyjny serwerowy (podstawowy) – 4 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	System operacyjny	Windows Server 2016 Standard Core MOLP GOV– fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika z nośnikiem i/lub licencją elektroniczną, wraz z serwerem należy dostarczyć wymaganą ilość licencji (16 rdzeni) – lub równoważny*. ***Przez równoważność zamawiający rozumie:** 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. 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. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. 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, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych

		wykorzystujących technologię ASP.NET. 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. login i hasło, b. karty z certyfikatami (smartcard), c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. 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), c. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, d. ustanawianie praw dostępu do zasobów domeny na

		bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, e. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. f. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. g. zdalna dystrybucja oprogramowania na stacje robocze. h. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. 26. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a. dystrybucję certyfikatów poprzez http, b. konsolidację CA dla wielu lasów domeny, c. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, d. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 27. Szyfrowanie plików i folderów. 28. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 29. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 30. Serwis udostępniania stron WWW. 31. Wsparcie dla protokołu IP w wersji 6 (IPv6), 32. Wsparcie dla algorytmów Suite B (RFC 4869), 33. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 34. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: a. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, b. obsługi ramek typu jumbo frames dla maszyn wirtualnych, c. obsługi 4-KB sektorów dysków, d. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, e. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, f. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode). 35. Możliwość automatycznej aktualizacji w oparciu o poprawki

		publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 36. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 37. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 38. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 39. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. **System musi współpracować z posiadanymi i wdrożonymi przez Zamawiającego w pełni usługami: min. Active Directory, DNS, DHCP. Zamawiający posiada wymagane licencje dostępowe MS CAL 2016.**

12. Oprogramowanie antywirusowe – min. 300 licencji.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Informacje ogólne	• Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10. • Wsparcie dla 32- i 64-bitowej wersji systemu Windows. • Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. • Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. • Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.
2.	Ochrona antywirusowa i antyspyware	• Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. • Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. • Wbudowana technologia do ochrony przed rootkitami. • Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. • Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. • Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. • 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. • 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). • Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. • Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. • Możliwość skanowania dysków sieciowych i dysków przenośnych. • Skanowanie plików spakowanych i skompresowanych. • Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. • Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku, ale również ma być możliwe użycie symbolu wieloznacznego „*" zastępującego dowolne znaki w ścieżce. • Administrator ma możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik. • Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. • Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. • Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas, co najmniej 10 min lub do ponownego uruchomienia komputera. • W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. • Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. • 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. • Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). • Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. • 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). • Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. • Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. • Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. • 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. • Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. • Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. • Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. • Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. • Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. • Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. • Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. • Procesy zweryfikowane, jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. • Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. • 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. • 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. • Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. • Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. • Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. • Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

		• Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. • Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. • 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. • Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. • Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. • 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. • 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. • System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. • System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. • Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu. • Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. • Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. • Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym, co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. • Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. • W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego

		nośnika. • Użytkownik ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika • Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). • Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: - tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, - tryb interaktywny, w którym to program 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 program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, - tryb inteligentny, – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. • Tworzenie reguł dla modułu HIPS musi odbywać się, co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. • Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. • Oprogramowanie musi posiadać zaawansowany skaner pamięci. • Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. • 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. • 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. • 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. • Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. • Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. • Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.

		• Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. • Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http. • Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). • Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). • Program ma być w pełni zgodny z technologią CISCO Network Access Control. • Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. • 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. • Użytkownik ma mieć możliwość skonfigurowania programu tak, aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. • Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. • Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. • Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. • Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. • Możliwość podejrzenia licencji za pomocą, której program został aktywowany. • W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór, co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych. Obsługa technologii Microsoft NAP. • W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. • Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. • Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostają przywrócone dotychczasowe ustawienia.

		• Administrator ma możliwość czasowego wstrzymania polityk, Wartości na liście wstrzymania czasowego podane są w minutach i godzinach. • Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. • Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki. • Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu. • Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. • Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji. • Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
3.	Ochrona antyspam	• Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. • Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. • Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. • Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. • Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. • Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. • Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej, jako spam. • Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook. • Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość, jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości, jako spam na automatyczne ustawienie jej właściwości, jako „przeczytana". • Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
4.	Zapora osobista (personal firewall)	• Zapora osobista ma pracować jednym z 4 trybów: - tryb automatyczny – program blokuje cały ruch przychodzący

		i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora, - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające, jaki ruch jest blokowany a jaki przepuszczany, - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu, w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. • Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący. • Możliwość tworzenia list sieci zaufanych. • Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. • Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. • Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. • Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. • Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. • Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. • Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. • Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. • Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. • Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. • Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. • Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. • Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. • Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie. • Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6.

		• Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. • Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. • Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o: - rozwiązanie problemów z aplikacją lokalną, którą wskazujemy z listy, - rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP.
5.	Kontrola dostępu do stron internetowych	• Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. • Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. • Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. • Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. • Aplikacja musi posiadać możliwość filtrowania url w oparciu, o co najmniej 140 kategorii i pod kategorii. • Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. • Moduł musi posiadać także możliwość grupowania kategorii już istniejących. • Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. • Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. • Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. • Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.
6.	Administracja zdalna	• Serwer administracyjny musi oferować możliwość instalacji na systemach min. Windows Server 2003, 2008, 2012 oraz systemach Linux. • Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). • Serwer administracyjny musi wspierać instalację w oparciu, o co najmniej bazy danych MS SQL i MySQL. • Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. • Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów

		oddzielnie bezpośrednio ze strony producenta. • Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. • Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. • Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. • Podczas logowania administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony panel zarządzający. • Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. • Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. • Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. • Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. • Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. • Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. • Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. • Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym. • Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. • Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. • Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. • Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. • Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. • Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. • Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. • Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. • Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. • Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nieposiadającymi zainstalowanego programu zabezpieczającego. • Agent musi przekazywać informacje na temat stanu systemu

		operacyjnego do serwera administracji zdalnej • .Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. • Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. • Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. • Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny. • Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. • W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. • Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. • Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. • Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. • Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. • Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. • Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej • Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. • Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. • Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. • Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. • Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. • Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po jakim użytkownik zostanie automatycznie wylogowany. • Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. • Zadania serwera obejmujące zadanie instalacji agenta, generowania

		raportów oraz synchronizacji grup. • Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. • Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. • Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań, jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji. • Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. • Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. • Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. • Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. • Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. • Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. • Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. • Grupy dynamiczne tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. • Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. • Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. • Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. • Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. • Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora. • Serwer administracyjny musi umożliwiać wyświetlenie polityk, do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta • Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.

		• Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. • Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. • Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp. • Serwer administracyjny musi oferować możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania. • Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. • Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. • Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. • Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. • Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. • Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. • Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. • Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. • Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. • Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. • Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. • Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. • Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. • Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. • Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.

		• Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. • Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. • Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie, co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. • Serwer administracyjny musi być wyposażony w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia, na jakim jest wyświetlana. • Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. • Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA. • Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie. • Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA. • Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar • Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy. • Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.
7.	Gwarancja/Ważność	Licencja na min. 300 stanowisk, na okres min. 5 lat.

13. Oprogramowanie do kopii bezpieczeństwa – 1 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Funkcjonalność	1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. 2. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. 3. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. 4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych

		wspieranych przez vSphere i Hyper-V. 5. Oprogramowanie musi być licencjonowane w modelu "per-CPU"lub innym umożliwiającym funkcjonowanie na dostarczonych serwerach przez Wykonawcę. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone. 6. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej 7. Oprogramowanie musi tworzyć "samowystarczalne" archiwa odnośnie odzyskania, do których niewymagana jest osobna baza danych z metadanymi deduplikowanych bloków. 8. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji 9. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie, dla co najmniej trzech pamięci masowych w takiej puli. 10. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. 11. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania. 12. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia. 13. Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki" na wirtualnej maszynie. 14. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware. 15. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time). 16. Oprogramowanie musi zapewniać bezpośrednią integrację

		z VMware vCloud Director 5.5, 5.6, 8.0, 8.10 i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.
		17. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
		18. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
		19. Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza.
		20. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
		21. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
		22. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
		23. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak, aby nieprzekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
		24. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
		25. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
		26. Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server.
		27. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
		28. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
		29. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
		30. Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione

		na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. 31. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu. 32. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych, jako źródła replikacji. 33. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik. 34. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn, jako źródła do dalszej replikacji (replica seeding). 35. Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V. 36. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN). 37. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere. 38. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing). 39. Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. 40. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania. 41. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować, jaką migrację swoimi mechanizmami. 42. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. 43. Oprogramowanie musi umożliwiać pełne odtworzenie

		wirtualnej maszyny bezpośrednio do Microsoft Azure. 44. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. 45. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 46. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: a. Linux • ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs b. BSD • UFS, UFS2 c. Solaris • ZFS, UFS d. Mac • HFS, HFS+ e. Windows • NTFS, FAT, FAT32, ReFS f. Novell OES • NSS 47. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. 48. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 49. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD. 50. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). 51. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.

		52. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. 53. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. 54. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. 55. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. 56. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows 57. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. 58. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. 59. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem. 60. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere. 61. Zamawiający wymaga dostarczenia licencji w ilości niezbędnej do poprawnej obsługi kopii zapasowych maszyn wirtualnych na dostarczonych serwerach.
2.	Konfiguracja/Instalacja	Oprogramowanie musi zostać zainstalowane przez Wykonawcę na serwerze Zamawiającego Dell R530 z konfiguracją kopii bezpieczeństwa uwzgledniającą maszyny z punktu: "1 Serwer rakowy – 2 szt."
3.	Gwarancja	Licencja musi być zgodna z serwerami Zaoferowanymi przez Wykonawcę z punktu:1 „Serwer rakowy – 2szt (4 procesory łącznie)". Min. 1 rok wsparcia świadczonego przez producenta rozwiązania, obejmującego dostęp do aktualizacji, nowych wersji oprogramowania i pomocy technicznej. Licencja bezterminowa (wieczysta) na używanie oprogramowania. **Zamawiający nie dopuszcza licencji subskrypcyjnych.**

1) **zgodnie z przepisami ustawy – Prawo zamówień publicznych oraz wg Wspólnego Słownika Zamówień CPV**

Część II.

Do Urzędu Miasta Zgierza należy dostarczyć, zainstalować i uruchomić następujące oprogramowanie bazodanowe według opisu przedmiotu zamówienia:

- Oprogramowanie bazodanowe (dostawa, instalacja, konfiguracja).

1. Oprogramowanie bazodanowe – 1 szt.

WARUNKI SZCZEGÓLNE:

LP.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Informacje ogólne-baza danych	Oracle Database Standard Edition 2 lub równoważny* Oracle WebLogic Server Standard Edition 12c lub równoważny* Oracle Forms and Reports 12c lub równoważny* **Wyżej wymienione oprogramowanie musi być ze sobą kompatybilne, nie dopuszczalne jest, żeby poszczególne elementy nie współpracowały między sobą.** ***Przez równoważność zamawiający rozumie:** **Równoważność dla Database Standard Edition 2:** 1.Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów PA-RISC i Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX), Intel/AMD Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach. 2.Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych. 3.Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego. 4.Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. 5.Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). 6.Możliwość migracji zestawu znaków bazy danych do Unicode. 7.Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych. 8.Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych. 9.Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych. 10.Wsparcie protokołu XA. 11.Wsparcie standardu JDBC 3.0. 12.Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.

		13.Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). 14.Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. 15.Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej). 16.Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych. 17.Baza danych powinna pozwalać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań. 18.Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik musi mieć aktywny dowolny podzbiór nadanych ról bazodanowych. 19.Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd) . Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online (hot backup). 20.Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. 21. Wsparcie dla klastra Active-Active. **Równoważność dla Oracle WebLogic Server Standard Edition 12c i Oracle Forms and Reports 12c:** 1. Funkcjonalność narzędzia klasy Middleware (oprogramowanie warstwy pośredniej infrastruktury IT), zapewniającego możliwość szybkiego tworzenia aplikacji z interfejsem użytkownika, polegającym na udostępnianiu formularzy wprowadzania danych, a następnie tworzenia raportów; możliwość pracy na danych, z co najmniej następujących źródeł: baza danych Oracle, JDBS, XML oraz pliki tekstowe. 2. Funkcjonalność narzędzia Rapid Application Development, wspomagającego programowanie w języku SQL, PL/SQL. 3. Wbudowany Serwer http. 4. Możliwość publikowania raportów do: przeglądarki internetowej, e-mail, WebDav, serwery ftp, lokalne systemy plików oraz

		z wykorzystaniem technologii Oracle Portal; 5. Wsparcie dla standardów J2EE w wersji 7: a) Batch Application Processing (JSR 352); b) Concurrent Manager Objects (JSR 236); c) domyślne źródła danych; d) JMS 2.0 Support for Simplified JMS Application Development (JSR 343); e) Java EE Connector Architecture 1.7 (JSR 322); f) Enterprise JavaBeans 3.2 (JSR-345); g) Clustering and High Availability Support for WebSocket 1.1 Applications; h) wsparcie kompresji GZIP w ramach kontenera WEB; i) Java EE 7 Security Standards; 6. Wsparcie dla technologii Multitenancy. 7. Wsparcie dla technologii Zero Downtime Patching polegającej na uproszczeniu procesu aktualizacji. 8. Zgodność z JDK 8. 9. Możliwość uruchamiania w kontenerze Docker. 10. Wsparcie dla technologii FastSwap. 11. Wsparcie dla następujących standardów Java. a) Batch Application Processing (JSR 352) 1.0; b) Contexts and Dependency Injection for Java EE 1.1; c) Dependency Injection for Java EE 1.0; d) Concurrent Managed Objects (JSR 236) 1.0; e) Expression Language (EL) 3.0, 2.2, 2.1, 2.0; f) Java API for JSON Processing (JSR-353) 1.0; g) Java API for XML-Based Web Services (JAX-WS) 2.2, 2.1, 2.0; h) Java API for RESTful Web Services (JAX-RS) 2.0; i) Java API for WebSocket 1.1; j) JavaBeans Activation Framework 1.1; k) Java EE 7.0; 1) Java EE Application Deployment 1.2; m) Java EE Bean Validation 1.1; n) Java EE Common Annotations 1.2; o) Java EE Connector Architecture 1.7; p) Java EE EJB 3.2, 3.1, 3.0, 2.1, 2.0, and 1.1; q) Java EE Enterprise Web Services 1.3, 1.2, 1.1; r) Java EE Interceptors 1.1; s) Java EE JDBC 4.0, 3.0; t) Java EE JMS 2.0, 1.1, 1.0.2b; u) Java EE JNDI 1.2; v) Java EE JSF 2.2, 2.1.*, 2.0, 1.2, 1.1; w) Java EE JSP 2.3, 2.2, 2.1, 2.0, 1.2, and 1.1; x) JSP 1.2. i 1.1 wraz z Expression Language (EL); y) Java EE Managed Beans 1.0; z) Java EE Servlet 3.1, 3.0, 2.5, 2.4, 2.3, and 2.2; aa) Java RMI 1.0; bb) JavaMail 1.4; cc) Java Transaction API 1.2; dd) JAX-B 2.2, 2.1,2.0;

		ee) JAX-P 1.3, 1.2, 1.1; ff) JAX-R 1.0; gg) JAX-RPC 1.1; hh) JDKs 8.0 (8.0 i 7.0 w przypadku klienta); ii) JMX 2.0; jj) JPA 2.1,2.0., 1.0; kk) JSR 77: Java EE Management 1.1; 12. JSTL1.2. mm) Managed Beans 1.0; nn) OTS/JTA OTS 1.2 i JTA 1.2; oo) RMI/IIOP 1.0; pp) SOAP Attachments for Java (SAAJ) 1.3, 1.2; qq) Streaming API for XML (StAX) 1.0; rr) Web Services Metadata for the Java Platform 2.0, 1.1; 13. Wsparcie dla następujących standardów: a) X.509 v3; b) LDAP v3; c) TLS vl.l, vi.2; d) HTTP 1.1; e) SNMP SNMPvl, SNMPv2, SNMPv3; f) xTensible Access Control Markup Language (XACML) 2.0; g) Partial implementation of Core and Hierarchical Role Based Access Control (RABC) Profile of XACML 2.0; h) Internet Protocol (IP) v6 v4;
2.	Gwarancja/Licencja	Licencjonowanie zgodne z serwerem Zamawiającego Dell R530 (Service Tag: D8Z9QK2) z min. parametrami 1xCPU, 8 rdzeni, parametry mogą ulec zmianie według złożonej oferty z min. ilością 50 użytkowników. Licencja musi umożliwiać zakładanie i kasowanie bez ograniczeń użytkowników w obrębie podanego parametru minimalnego (min. 50) . W przypadku zaoferowania licencji typu „Application Specific Full Use" oprogramowanie bazodanowe musi umożliwiać uruchomienie w swoim środowisku bazodanowym System Informatycznego URZĄD.NT firma Sputnik Software Sp. z o.o., 60-201 Poznań, ul. Górecka 30. Oprogramowanie dostarczone na nośniku zewnętrznym lub z możliwością pobrania z Internetu pakietu instalacyjnego przez Zamawiającego. Gwarancja min. 1 rok, usługa wsparcia technicznego musi być świadczona przez serwis producenta oprogramowania.
3.	Konfiguracja/Instalacja	Oprogramowanie musi zostać zainstalowane przez Wykonawcę na serwerze Zamawiającego Dell R530 z konfiguracją pozwalającą na jego uruchomienie i optymalne działanie.

1) **zgodnie z przepisami ustawy – Prawo zamówień publicznych oraz wg Wspólnego Słownika Zamówień CPV**

SPORZĄDZIŁ:

NACZELNIK WYDZIAŁU ZAMAWIAJĄCEGO:

SEKRETARZ MIASTA

Zgierz, 26.07.2018

(podpis, pieczątka)

Robert Chocholski

(podpis, pieczątka)