

OPIS PRZEDMIOTU ZAMÓWIENIA

SPIS TREŚCI

Wstęp 3

Wymagania minimalne 4

Serwer	4
Modernizacja posiadanego serwera na potrzeby serwera backupu danych	6
Przełączniki – typ I	6
Przełącznik – typ II	8
Przełącznik – typ III	10
Stacja robocza	11
Skaner dokumentów do obiegu dokumentów	15
Zestaw wideokonferencji do transmisji posiedzeń rady	16
Urządzenie klasy UTM	18
Oprogramowanie do monitorowania sieci i pracowników	22
Certyfikowane szkolenie dla administratora z dostarczonego urządzenia klasy UTM	28

Wymagania dodatkowe 29

Wstęp

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowa Gmina” realizowanego przez Gminę Gizałki.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina” dla Gminy Gizałki o numerze POPC.05.01.00-00-0001/21-00.

Wymagania minimalne

Serwer

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Obudowa rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor 12-rdzeniowy, min. 3.0 GHz (Turbo Speed min. 3.6 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 28500 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/ wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim.
RAM	128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum dwa sloty PCIe z czego przynajmniej jeden generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowa dwuportowa karta 10GbE BaseT
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane: 6 dysków SAS o pojemności min. 900GB, 12Gb, 15K, Hot-Plug, Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 600W każdy
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twarde. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

	• Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	• Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub inną równoważną Serwer musi posiadać deklarację CE lub inną równoważną
Warunki gwarancji	60 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia Zamawiający wymaga dołączenia do oferty poświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 lub inną równoważną na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty poświadczenia, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Rekonfiguracja systemów i szkolenie z dostarczonego rozwiązania	W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług: 1) rekonfiguracja serwera: - montażu w/w sprzętu w szafach rack Zamawiającego w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. - aktualizacja do najnowszych wersji oprogramowania układowego serwera i jego komponentów

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	- podłączenia serwera do przełącznika za pomocą właściwych kabli zapewniającego bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera - testów niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania 2) Szkolenie z dostarczonego rozwiązania na miejscu u Zamawiającego. Zakres tematyczny: - omówienie fizycznych interfejsów sprzętu - sposoby podłączenia kart rozszerzeń (np. dodatkowych kart) - konfiguracja kontrolera pamięci masowej, tworzenie RAID - ustawienia BIOS - bezpieczeństwo - przeprowadzenia szkolenia z zarządzania niskopoziomowego dostarczanych serwerów obejmującą: • tworzenie grup RAID • obsługę wirtualnej konsoli (podłączanie napędów ISO) • diagnozowanie ewentualnych problemów • generowanie logów Zamawiający wymaga, aby wszystkie usługi zostały zrealizowane przez inżyniera rozwiązania serwerowego posiadającego certyfikację producenta dostarczonego serwera poświadczającą wiedzę z zakresu oferowanego sprzętu – dokumenty dołączyć do oferty.
Ilość	1 kpl.

Modernizacja posiadanego serwera na potrzeby serwera backupu danych

Nazwa	Minimalne wymagania dla sprzętu
Typ	Rozbudowa posiadanej infrastruktury serwerowej
Wymagania minimalne	W ramach modernizacji Wykonawca zobowiązany jest do dostarczenia komponentów do: - Rozbudowy posiadanego przez Zamawiającego jednego serwera o kompatybilne 4 dyski o pojemności min 8TB, 7,5K obr./min, samoszyfrujące, typu Hot-Plug, 3,5" - Dell PowerEdge R430 o numerze seryjnym 8C46RG2 wraz z gwarancją producenta na min. 24 miesiące. - Rozbudowy posiadanego przez Zamawiającego jednego serwera o kontroler BOSS Card PCIe oraz 2 szt. dysków M.2 o pojemności minimum 240 Gb: - Dell PowerEdge R430 o numerze seryjnym 8C46RG2 wraz z gwarancją producenta na min. 24 miesiące.
Ilość	1 kpl.

Przełączniki – typ I

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Do montażu w szafie rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 48 porty 10/100/1000Mbps RJ45, minimum 2 porty SFP/SFP+ 1/10GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 8000 adresów MAC Switch fabric capacity min. 100Gbps Forwarding rate min. 100Mpps

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	Pamięć flash min. 128MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Możliwość połączenia w stos do 4 urządzeń tego samego typu Wydajność połączenia pomiędzy przełącznikami w stosie min. 20Gbps Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIPv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIPv2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIPv2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9) 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Inne	Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza
Wypożyczenie dodatkowe	Zamawiający wymaga, aby wraz z przełącznikiem typ I zostało dostarczone okablowanie: - 4 szt. moduły światłowodowe wielomodowe 1GbE SX - 4 szt. patchcord LC/UPC-SC/UPC Duplex OM3 3m - 4 szt. adapter światłowodowy SC duplex MM, OM3
Wdrożenie	W ramach dostawy sprzętu Wykonawca zobowiązany jest także do przeprowadzenia wdrożenia dostarczanego przełącznika, które musi objąć zakres minimum: - fizyczny montaż i adresację - konfigurację do 5 wirtualnych sieci (VLAN). - segmentację sieci z podziałem na sieć do zarządzania oraz sieć lan - wykonanie jednej spójnej dokumentacji sieci w wdrażanego urządzenia (urządzeń sieciowych) w ramach całego postępowania.
Gwarancja	dożywotnia (gwarancja producenta)
Ilość	1 kpl.

Przełącznik – typ II

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Do montażu w szafie rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 24 porty 10/100/1000Mbps RJ45, minimum 2 porty SFP/SFP+ 1/10GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX Obsługa modułów SFP+: 10GbE, SR, LR, ER
Wydajność przełącznika	Minimum 8000 adresów MAC Switch fabric capacity min. 80Gbps Forwarding rate min. 80Mpps Pamięć flash min. 128MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Możliwość połączenia w stos do 4 urządzeń tego samego typu Wydajność połączenia pomiędzy przełącznikami w stosie min. 20Gbps Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIV1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIV2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIV2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9) 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSh Public Key File Format 6101 SSL
Inne	Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza
Wdrożenie	W ramach dostawy sprzętu Wykonawca zobowiązany jest także do przeprowadzenia wdrożenia dostarczanego przełącznika, które musi objąć zakres minimum: - fizyczny montaż i adresację.
Gwarancja	dożywotnia (gwarancja producenta)
Ilość	1 szt.

Przełącznik – typ III

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	Do montażu w szafie rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
Porty	Minimum 8 portów 10/100/1000Mbps RJ45, minimum 2 porty SFP 1GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX
Wydajność przełącznika	Minimum 8000 adresów MAC Switch fabric capacity min. 17Gbps Forwarding rate min. 10Mpps Pamięć flash min. 128MB
Funkcjonalność warstwy II	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
Inne Funkcjonalności	Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa	1155 SMIPv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIPv2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIPv2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9) 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
Inne	Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza
Wdrożenie	W ramach dostawy sprzętu Wykonawca zobowiązany jest także do przeprowadzenia wdrożenia dostarczanego przełącznika, które musi objąć zakres minimum: - fizyczny montaż i adresację.
Gwarancja	dożywotnia (gwarancja producenta)
Ilość	1 szt.

Stacja robocza

Nazwa	Minimalne wymagania dla sprzętu
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Wydajność obliczeniowa	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 12 300 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php - wydruk należy dołączyć do oferty. Dopuszcza się wydruk w języku angielskim.
Pamięć RAM	8GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB.
Pamięć masowa	Dysk M.2 SSD 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5" lub 3.5"
Wydajność grafiki	Zintegrowana z procesorem
Wypożyczenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5" lub 1 x dysku 2.5" wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez

	konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnek zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiorem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiągniętej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z wewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym hasle administratora. Użytkownik po wpisaniu swojego hasła jest w stanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z

	serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi
System operacyjny	Zainstalowany system operacyjny spełniający następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Licencja bezterminowa zapewniająca prawo do wykorzystywania przez jednostki samorządu terytorialnego. 2. Polska wersja językowa. 3. System operacyjny powinien być dostarczony w najnowszej oferowanej przez producenta wersji. 4. Aktualizacje funkcji dla systemu operacyjnego. 5. Obsługa procesorów wielordzeniowych. 6. Graficzny okienkowy interfejs użytkownika. 7. Obsługa co najmniej 8 GB RAM. 8. Dostęp do aktualizacji w ramach zaoferowanej wersji systemu operacyjnego przez Internet bez dodatkowych opłat. 9. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. Możliwość przystosowania stanowiska dla osób niepełnosprawnych: • lupa powiększająca zawartość ekranu, • narrator odczytujący zawartość ekranu, • regulacja jasności i kontrastu ekranu, • możliwość odwrócenia kolorów np. biały tekst na czarnym tle, • poprawa widoczności elementów ekranu np. regulowanie grubości kursora myszy - małej strzałki na ekranie, wskazującej lokalizację myszy i czasu trwania powiadomień systemowych, • funkcja sterowania myszą z klawiatury numerycznej, • funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza, • korzystanie z wizualnych rozwiązań alternatywnych wobec dźwięków, • funkcja napisów w treściach wideo, • możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków; 13. Możliwość zarządzania stacją roboczą poprzez polityki. 14. System musi posiadać narzędzia służące do administracji, wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 15. Wsparcie dla min. Sun Java i .NET Framework 1.1 i 2.0 i 3.0 i 4.5 – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. 16. Wsparcie dla min. JScript i VBScript - możliwość uruchamiania interpretera poleceń. 17. 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. 18. Graficzne środowisko instalacji i konfiguracji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników. 20. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.

Finansowano w ramach reakcji Unii na pandemię COVID-19

	21. Oprogramowanie dla tworzenia kopii zapasowych, automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 22. Możliwość przywracania plików systemowych. Możliwość identyfikacji sieci komputerowych, do których jest podłączony komputer, zapamiętywania ustawień i przypisywania do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
Certyfikaty i standardy	• Certyfikat ISO9001 lub inny równoważny dla producenta sprzętu • Certyfikat ISO 14001 lub inny równoważny dla producenta sprzętu • Certyfikat ISO 50001 lub inny równoważny dla producenta sprzętu • Deklaracja zgodności CE lub równoważny • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych • Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym
Wymagania dodatkowe	Wbudowane porty: 2x Display Port 1.4, port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w tym min 2 porty USB na przednim panelu obudowy i min. 4 porty USB 3.2 gen. 1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Monitor	Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8" (16:9) Technologia wykonania matrycy: IPS Jasność 250 cd/m2 Kontrast Typowy 1000:1 Kąty widzenia (pion/poziom): 178/178 stopni Czas reakcji matrycy: max. 8 ms Rozdzielczość maksymalna: 1920 x 1080 przy 60Hz Powłoka powierzchni ekranu: Antyodblaskowa utwardzona Podświetlenie: System podświetlenia LED Bezpieczeństwo: Monitor musi być wyposażony w tzw. gniazdo zabezpieczenia przed kradzieżą. Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie. Złącza min.: 1x D-Sub, 1x Display Port 1.2 Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub inną równoważną oraz wykazana zgodnie z normą ISO 9296 lub inną równoważną w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 26 dB (załączyć do oferty dokumenty potwierdzające).
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Minimum 36 miesięczna gwarancja producenta świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego

	Firma serwisująca musi posiadać ISO 9001: 2015 lub inną równoważną na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera – dokumenty poświadczające załączyć do oferty. Do oferty należy załączyć dokumenty poświadczające, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, producent przejmie na siebie wszelkie zobowiązania związane z serwisem. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Zamawiający wymaga dołączenia dokumentów poświadczających, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Dodatkowe oprogramowanie	Oprogramowanie zarządzające producenta komputera, zainstalowane na etapie produkcji komputera, umożliwiające min.: - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu - powiadomienie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, jakiego komponentu sprzętu dotyczy aktualizacja, wszystkich poprzednich aktualizacjach z informacjami jak powyżej. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Ilość	1 kpl.

[Skaner dokumentów do obiegu dokumentów](#)

Nazwa	Minimalne wymagania dla sprzętu
-------	---------------------------------

Typ skanera (obudowa)	Kompaktowy skaner A4
Sposoby skanowania	Funkcja automatycznego skanowania z podajnikiem ADF, skanowanie dwustronne
Obsługiwane formaty (nie złożone na pół)	Minimum w zakresie A4, koperta, plastikowe karty identyfikacyjne
Szybkość skanowania (dla dokumentów A4 200 dpi / 300 dpi)	Jednostronny minimum: 60 str./min Dwustronny minimum: 120 obr./min
Pojemność ADF	80 arkuszy (A4: 80 g/m ²)
Dzienna przepustowość	Minimum 4 000 stron
Wyjściowa głębia kolorów	Kolor minimum: 24-bity, skala szarości: 8-bitów, monochromatyczny: 1-bit
Optyczna rozdzielczość skanowania	Minimum 600 DPI x 600 DPI
Dodatkowe funkcje skanowania	- Wiele obrazów - pomijanie pustej strony - automatyczny kolorowy - kadrowanie i odkrzywianie - usuwanie dziurek - kadrowanie tabulatur - oddzielanie góry i dołu - dyfuzja błędów - usuwanie mory - podkreślanie obrazu - oczyszczanie kolorów - usuwanie kolorów (R, G, B, brak, biały, wskazany, nasycenie kolorów) - naprawa krawędzi - redukcja pasów w pionie
Tryby koloru skanowania	Monochromatyczny, odcienie szarości, kolor
Typ i gramatura papieru	Zwykły papier, cienki papier, gruby papier, papier makulaturowy, wizytówka, Karty plastikowe
Obsługiwane systemy operacyjne	Windows 7/10 (32/64-bit) posiadane przez Zamawiającego oraz systemy operacyjne dostarczone ze stacjami roboczymi (dostarczone w ramach niniejszego postępowania)
Interfejsy komunikacyjne	Min. 1 x USB 3.0 (kompatybilność wsteczna)
Gwarancja	Minimum 24 miesięcy gwarancji producenta urządzenia

Zestaw videokonferencji do transmisji posiedzeń rady

Nazwa	Minimalne wymagania dla sprzętu
System telekonferencyjny audio	Na zestaw systemu telekonferencyjny audio musi się składać minimum: 1) Jednostka centralna systemu konferencyjnego (1 szt.), która musi posiadać: - Możliwość podłączenia i zasilania minimum 50 pulpitów mikrofonowych (2 x 25) - wbudowany głośnik oraz wyjście słuchawkowe - możliwość wyboru trybu pracy: minimum ograniczona liczba mówców, ograniczony czas wypowiedzi, tylko przewodniczący - blokada klawiszy - wyświetlanie daty/czasu, czasu do końca wypowiedzi, funkcja testowania podłączonych pulpitów mikrofonowych - możliwość rozbudowania sekcji połączeniowej dla dodatkowych urządzeń np. mikrofonów, centrali telefonicznej, procesorów sygnałowych (np. korektora), rejestratorów, wzmacniaczy, źródeł liniowych audio

	2) Okablowanie (1 szt.): - kabel przedłużający 7-pinowy wtyk DIN na 7-pinowe gniazdo DIN Długość: minimum 10m 3) Mikrofon konferencyjny Przewodniczącego (1 szt.), który musi umożliwiać: - włączenie pulpitu mikrofonowego przewodniczącego - musi posiadać wkładkę mikrofonową typu back electret o charakterystyce kardiodoidalnej - musi posiadać wbudowany głośnik - musi posiadać możliwość podłączenia słuchawek - musi posiadać przycisk aktywujący dla wygodnego użytkownika - musi umożliwiać wyświetlenie statusu pracy sygnalizowany za pomocą diody na mikrofonie - musi posiadać przycisk priorytetu do przerywania wypowiedzi delegatów oraz emisji gongu 4) Mikrofon konferencyjny Delegata (17 szt.), który musi umożliwiać: - włączenie pulpitu mikrofonowego delegata - musi posiadać wkładkę mikrofonową typu back electret o charakterystyce kardiodoidalnej - musi posiadać wbudowany głośnik - musi posiadać możliwość podłączenia słuchawek - musi posiadać przycisk aktywujący dla wygodnego użytkownika - musi umożliwiać wyświetlenie statusu pracy sygnalizowany za pomocą diody na mikrofonie 5) Podwójny odbiornik wieloczęstotliwościowy (1 szt.), o wymaganiach minimalnych: - musi zawierać podwójny odbiornik wieloczęstotliwościowy, w technologii minimum UHF PLL - musi posiadać możliwość wyboru minimum 2 x 1000 kanałów UHF (672.000-696.975MHz), podzielonych na 10 grup po 100 - musi posiadać funkcję ACT do przesyłania wybranej częstotliwości w podczerwieni do nadajnika minimum TXS-606LT, TXS-606HSE lub mikrofonów TXS-606HT i TXS-606DT - musi posiadać automatyczne wyszukiwanie częstotliwości - musi posiadać próg wyciszenia szumów (squellch) i regulację głośności dla każdego kanału - musi posiadać wyświetlacz LCD dla każdej sekcji: grupa/kanał, antena A/B, poziom mocy sygnału RF, poziom sygnału audio - musi posiadać dodatkowy wskaźnik poziomu audio - zasilacz 6) Mikrofon bezprzewodowy doreczny (2 szt.), który musi posiadać: - wbudowany nadajnik wieloczęstotliwościowy w technologii minimum UHF PLL - dynamiczną wkładkę mikrofonową (kardiodoida) - możliwość wyboru 1000 kanałów UHF (672.000-696.975MHz), synchronizacja z odbiornikami TXS-606, TXS-626, TXS-646 oraz TXS-686 poprzez - regulowaną czułość - przełączaną moc nadajnika (high: 25mW/low: 2.5mW) - wyświetlacz LCD pokazujący minimum: grupa/kanał, poziom sygnału audio i stan baterii - zasilanie: 2 x 1.5V bateria AA
Zestaw do transmisji	Na zestaw do transmisji musi się składać minimum: 1) Kamera IP (1 szt.) o wymaganiach minimalnych: - rozdzielczość minimum: 1920x1080 / 50kl/s - interfejs: Ethernet 10/100 Base-T PoE 802.3af - ilość pikseli: 2Mpx - czułość minimum: kolor: 0.004lux/F1.2-1/3s 30IRE, 0.04lux/F1.2-1/30s 30IRE B/W: 0.002lux/F1.2-1/3s 30IRE, 0.02lux/F1.2-1/30s 30IRE - mechaniczny filtr podczerwieni ICR - wbudowany mikrofon - rozbudowane funkcje inteligentnej analizy obrazu (IVS) - obsługa kart microSD / microSDHC / microSDXC do 128GB - zgodność ze standardem: ONVIF, CGI, Milestone, Genetec, RTSP, - port RS485 - wejścia/wyjścia audio minimum: 1/1 - wejścia/wyjścia alarmowe minimum: 2/1

Finansowano w ramach reakcji Unii na pandemię COVID-19

	- obsługa technologii ePoE minimum: (800m - 10Mb/s, 300m - 100Mb/s) 2) Karta pamięci (1 szt.) o wymaganiach minimalnych: - pojemność minimum: 64 Gb - prędkość odczytu minimum: 100MB/s 3) Obiektyw megapikselowy (1 szt.), o wymaganiach minimalnych: - regulowana ogniskowa obiektywu: 2.8 - 12mm - wielkość przetwornika: minimum 1/2.7" - jasność: minimum F1.4 - mocowanie: CS - maksymalna rozdzielczość: 3MPx - pierścień do regulacji ostrości oraz ogniskowe 4) Przenośny statyw z uchwytem do kamery kompaktowej (1 szt.) 5) Zasilacz POE do kamery IP (1 szt.), o wymaganiach minimalnych: - zasięg transmisji: do minimum 100m - zasilanie: 100~240V AC, 50~60Hz - napięcie wyjściowe: 48~52V DC - moc wyjściowa: ≤15,4W - kompatybilny z standardem: IEEE802.3af 6) Okablowanie: - 1 x kabel audio minimum 20m, umożliwiający połączenie dostarczonego systemu konferencyjnego z kamerą do transmisji - 1 x patchcord UTP minimum kat. 6 kabel sieciowy LAN 2x RJ45 minimum 20m do podłączenia kamery z siecią LAN - 1 x kabel HDMI minimum 15 m
Gwarancja	Min. 12 miesięcy
Ilość	1 kpl.

Urządzenie klasy UTM

Nazwa	Minimalne wymagania dla urządzenia
Typ	Urządzenie klasy UTM wraz z niezbędnymi serwisami i aktualizacjami oraz wdrożeniem i szkoleniem
Wymagania techniczne	Dostarczone urządzenie klasy UTM musi posiadać następujące minimalne funkcje: - Obsługa sieci w zakresie minimum: Urządzenie musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. - Zapora korporacyjna musi posiadać minimum: • Urządzenie musi być wyposażone w Firewall klasy Stateful Inspection. • Urządzenie musi obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. • Urządzenie musi dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). • Firewall musi posiadać interfejs GUI w formie interfejsu dostępnego z przeglądarki internetowej (WebGUI). • Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów, adresów IP, użytkownika bądź grupy bazy z lokalnej bazy użytkowników, LDAP lub Active Directory. • Firewall musi umożliwiać wyszukiwanie w zdefiniowanych przez administratora politykach bezpieczeństwa. • Firewall musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP. - INTRUSION PREVENTION SYSTEM (IPS) w zakresie minimum: • System detekcji i prewencji włamań (IPS) ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów oraz analizy w oparciu o sygnatury kontekstowe.

	• Urządzenie musi posiadać moduł wykrywania typu lub nazwy aplikacji, której ruch jest filtrowany przez urządzenie. • Moduł skanujący musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. • Moduł IPS musi pozwalać na automatyczne blokowanie wykrytych ataków. • Urządzenie musi mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. • Administrator urządzenia musi mieć możliwość konfiguracji trybu inspekcji ruchu IPS lub jego wyłączenia dla danej polityki bezpieczeństwa. • Urządzenie musi zapewniać możliwość tworzenia wykluczeń dla systemu IPS. • System IPS musi klasyfikować zagrożenia co najmniej na poziomach Niski (np. Low, Minor) oraz Wysoki (np. High, Major). • Urządzenie musi mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem. 4. Kształtowanie pasma (Traffic Shapping) w zakresie minimum: • Urządzenie musi mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. • Ograniczenie pasma lub priorytetyzacja musi być określana względem adresu IP, pola DSCP, polityki bezpieczeństwa, aplikacji. 5. Ochrona antywirusowa w zakresie minimum: • Rozwiązanie musi zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). • Co najmniej jeden z dwóch skanerów antywirusowych musi być dostarczany w ramach podstawowej licencji. • Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. • W okresie gwarancji musi być możliwość korzystania z dowolnego z wybranych skanerów antywirusowych z aktualizowaną bazą sygnatur 6. Ochrona antyspam w zakresie minimum: • Producent musi udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). • Ochrona antyspam musi działać w oparciu o: 1. białe/czarne listy, 2. DNS RBL lub RPD (Recurrent Pattern Detection), 3. W przypadku ochrony DNS RBL rozwiązanie powinno posiadać także heurystyczny skaner. 4. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 5. Rozwiązanie musi dodawać odpowiedni wpis w nagłówku wiadomości zaklasyfikowanej jako spam. 7. WIRTUALNE SIECI PRYWANTE (VPN) minimum: • Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). • Odpowiednio kanały VPN można budować w oparciu o: a. IPSec VPN, b. SSL VPN • SSL VPN musi działać w trybach Tunel i Portal. • W ramach funkcji SSL VPN producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. • Urządzenie musi posiadać funkcjonalność przełączenia tunelu na łączy zapasowe na wypadek awarii łączy dostawcy podstawowego (VPN Failover). • Urządzenie musi posiadać wsparcie dla technologii Hub 'n' Spoke. • Urządzenie musi umożliwiać tworzenie tuneli w oparciu o technologię Route Based. 8. Filtr dostępu do stron WWW w zakresie minimum: • Urządzenie musi posiadać wbudowany lub chmurowy filtr URL.
--	--

	- Filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 40 kategorii tematycznych stron internetowych. - Administrator musi mieć możliwość tworzenia wykluczeń stron z Filtra URL. - Administrator musi posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z co najmniej dwóch akcji: - blokowanie dostępu do adresu URL, - zezwolenie na dostęp do adresu URL. - Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. - Urządzenie musi posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 9. Uwierzytelnianie w zakresie minimalnym: - Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: - lokalną bazę użytkowników, - zewnętrzną bazę użytkowników (zewnętrzny LDAP), - usługę katalogową Microsoft Active Directory. - Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia - autoryzację w oparciu o: - wbudowaną bazę użytkowników, - LDAP lub Active Directory, - Radius, - Urządzenie musi udostępniać mechanizm transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 10. Administracja łączami do internetu (isp) w zakresie minimalnym: - Urządzenie musi posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). - Mechanizm równoważenia łączy musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. - Urządzenie musi posiadać mechanizm przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego. - Urządzenie musi posiadać mechanizm statycznego trasowania pakietów. - Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego. - Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. - Rozwiązanie musi zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 11. Dodatkowe wymagania minimalne: - Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. - Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. - Konfiguracja serwera DHCP musi być możliwa dla protokołu IPv4 i IPv6. - Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. - Urządzenie musi być wyposażone w możliwość konfiguracji usługi SNMP w wersji 2 i 3. - Urządzenie musi posiadać usługę DNS Proxy. 12. Administracja urządzeniem – wymagania minimalne: - Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. - Komunikacja może odbywać się na porcie innym niż https (443 TCP). - Urządzenie musi być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. - Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
--	---

	• Urządzenie musi mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). • Rozwiązanie musi mieć możliwość eksportowania logów za pomocą protokołu IPFIX lub NetFlow. • Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji). 13. Raportowanie – zakres minimalny: • Urządzenie powinno zostać dostarczone z systemem raportowania i przeglądania logów w postaci wbudowanej w urządzenie lub w postaci zewnętrznego oprogramowania oferowanego przez producenta urządzenia wraz z niezbędnym sprzętem do uruchomienia tego rozwiązania. • Powinno zostać udostępnione co najmniej 128GB pamięci na logi i raporty o wydajności wymaganej przez producenta urządzenia. • Logi i raporty nie mogą być przechowywane w chmurze. Wymagane jest rozwiązanie przechowywania lokalnego. • System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego (mail). • System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów. • W ramach podstawowej licencji zamawiający musi otrzymać możliwość korzystania z systemu zbierania logów i tworzenia raportów. • Dodatkowy system umożliwia tworzenie raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy 14. Parametry minimalne dla sprzętu: • Liczba portów Ethernet 10/100/1000Mbps – min.8. • Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą połączeń LTE za pomocą wbudowanego modemu lub zewnętrznego modemu z interfejsem USB. • Przepustowość Firewall – min. 2 Gbps. • Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min. 1.3 Gbps. • Przepustowość filtrowania Antywirusowego – min. 400 Mbps. • Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps. • Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 50. • Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20. • Obsługa min. VLAN 64. • Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15000 nowych sesji/sekundę. • Urządzenie nie może być Nielimitowane na użytkowników.
Dodatkowe wymagania	Urządzenie w żadnym zakresie technologicznym nie może się opierać na rozwiązaniach sprzętowych lub programowych będących w konflikcie z ustawą o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego
Wdrożenie	W ramach wdrożenia Wykonawca zobowiązany jest do przeprowadzenia prac wdrożeniowych z zakresie minimum: -Wstępna konfiguracja urządzenia (zaadresowanie interface'ów, konfiguracja routingu, DNS, NTP), -Konfiguracja profili administracyjnych, - Podpięcie weryfikacja statusu licencji, -Konfiguracja obiektów adresowych na potrzeby polityk Firewall (na podstawie przygotowanej wcześniej listy), -Konfiguracja polityk Firewall pomiędzy strefami bezpieczeństwa, -Weryfikacja komunikacji pomiędzy strefami bezpieczeństwa, -Konfiguracja lokalnej bazy użytkowników oraz zdefiniowanie grup, oraz podłączenie do usługi LDAP/AD - Konfiguracja VPN wg potrzeby -Konfiguracja IPSec VPN site-to-site, -Konfiguracja IPSec VPN client-to-site, -Konfiguracja SSL VPN client-to-site, -Konfiguracja profili kontroli Antywirusowej i podpięcie do polityk FW, -Konfiguracja profili ochrony przed atakami IPS i podpięcie do polityk FW, -Konfiguracja profili kontroli aplikacji i podpięcie do polityk FW, -Konfiguracja profili kontroli WWW i podpięcie do polityk FW,

	-Konfiguracja profili antyspamowych i podpięcie do polityk FW, -Test zastosowanych funkcji ochronnych, -Przygotowania ogólnej dokumentacji z zakresu zdefiniowanych funkcji. Instruktaż: Wymagane jest, aby wdrożenie oraz instruktaż został wykonany przez inżynierów certyfikowanych przez producenta dostarczonego rozwiązania klasy UTM w minimalnym zakresie: -Przeszkolenie z zakresu zarządzania wszystkimi elementami podlegającymi konfiguracji w punkcie "Wdrożenie" -Szkolenie musi trwać minimum 3h -Szkolenie z odtwarzania konfiguracji po awarii urządzenia backup lokalny/backup z chmury producenta. -Przeszkolenie z zakresu prostych narzędzi do rozwiązywania problemów. Dodatkowo Wykonawca ma zapewnić wsparcie powdrożeniowe przez okres minimum 3 lat, w każdym miesiącu do wykorzystania 2 godziny przez Zamawiającego. W ramach wsparcia wymagane jest udostępnienie Zamawiającemu dostępu do portalu typu helpdesk, który to będzie umożliwiał zakładanie zgłoszeń serwisowych online. W razie potrzeby może być wymagane zdalne podłączenie się do infrastruktury zamawiającego np. przez VPN lub aplikacje do zdalnej pomocy technicznej. W ramach dostawy wymagane jest także dostarczenie wraz z urządzeniem klasy UTM półki do szafy rackowej „19” lub dedykowanego uchwytu do szafy rackowej „19”.
Gwarancja	Wymaga się, aby dostawa obejmowała również minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu oraz licencje dla wszystkich funkcji bezpieczeństwa.
Ilość	1 szt.

Oprogramowanie do monitorowania sieci i pracowników

Nazwa	Minimalne wymagania dla sprzętu
Wymagania ogólne	- Oprogramowanie musi umożliwiać ewidencjonowanie zasobów w szczególności: osób, komputerów, serwerów fizycznych, maszyn wirtualnych, urządzeń infrastruktury sieciowej, monitorów, drukarek, urządzeń mobilnych, nośników danych, numerów telefonów, systemów informatycznych, oprogramowania, licencji, umów. - Oprogramowanie musi zapewniać zaewidencjonowanie minimum 150 zasobów w bazie CMDB tj.: komputery, serwery, maszyny wirtualne, urządzenia sieciowe, drukarki, telefony/tablety. - Oprogramowanie musi posiadać widok zbiorczy wszystkich zasobów prezentujący liczbę zasobów w każdej grupie z podziałem na statusy, w szczególności aktywne oraz nieaktywne. - Oprogramowanie musi umożliwiać tworzenie relacji wiążących zasoby między sobą w logiczny sposób np. właściciel komputera, przełożony pracownika, licencja przypisana na prawie per user lub per device. - Oprogramowanie musi posiadać mechanizm tworzenia schematu organizacyjnego w strukturze drzewiastej z możliwością opisanie m.in. szefa działu, numeru MPK itp. - Oprogramowanie musi posiadać mechanizm tworzenia schematu lokalizacji w strukturze drzewiastej z możliwością opisanie m.in. zarządcy budynku, adresu. - Oprogramowanie musi posiadać możliwość przypisywania zasobów do schematu organizacyjnego oraz lokalizacji. - Oprogramowanie musi posiadać możliwość integracji z wieloma kontrolerami domeny AD/LDAP. - Oprogramowanie musi posiadać mechanizm automatycznego przypisywania osób do schematu organizacyjnego na podstawie kont w AD/LDAP. - Oprogramowanie musi posiadać mechanizm wyszukiwania danych metodą full-text-search na podstawie wpisanej frazy. - Oprogramowanie musi posiadać możliwość budowania zaawansowanych filtrów dla zasobów, dostępnych dla wybranych użytkowników lub całej organizacji. - Oprogramowanie musi posiadać mechanizm importu i aktualizacji danych z plików płaskich CSV, wraz z możliwością pobrania przykładowych plików wzorcowych.

	13. Oprogramowanie musi posiadać możliwość eksportowania danych do plików płaskich CSV. 14. Oprogramowanie musi umożliwiać konfigurację serwera poczty SMTP. 15. Oprogramowanie musi posiadać możliwość ustawienia powiadomień w konsoli oprogramowania oraz wysyłanych na pocztę e-mail, z możliwością konfiguracji dla określonej osoby / grupy osób, w szczególności o: zainstalowaniu oprogramowania na komputerze, nadchodzącym i przekroczonym terminie gwarancji zasobu, nadchodzącym i planowanym terminie wymiany zasobu, nadchodzącej i przekroczonej dacie końca wsparcia producenta zasobu, nadchodzącym i przekroczonym terminie ważności zasobu typu licencja, nadchodzącej i przekroczonej dacie aktywacji licencji, 16. Oprogramowanie musi posiadać mechanizm tworzenia ról składających się z uprawnień do czynności wykonywanych przez użytkowników w oprogramowaniu. 17. Oprogramowanie musi umożliwiać przypisywanie ról do użytkowników w szczególności w taki sposób, aby osoby z działu X miały automatycznie rolę Y w oprogramowaniu. 18. Oprogramowanie musi posiadać predefiniowane role systemowe, w szczególności administrator systemu, administrator biznesowy, osoba zarządzająca CMDB. 19. Oprogramowanie musi posiadać możliwość logowania użytkowników do oprogramowania za pomocą poświadczeń AD/LDAP. 20. Oprogramowanie musi posiadać możliwość grupowego dodawania zasobów z poziomu jednego ekranu aplikacji: komputerów, serwerów, urządzeń sieciowych, licencji, urządzeń mobilnych, drukarek, bez względu na producenta, markę i model, z możliwością wpisania cech unikatowych: numer seryjny, numer licencji czy termin gwarancji. 21. Oprogramowanie musi posiadać możliwość automatycznego uzupełniania informacji o szczegółach komputera na podstawie słownika produktów handlowych w szczególności: producenta, modelu, typu procesora, wielkości pamięci RAM oraz pojemności dysku twardego. 22. Oprogramowanie musi umożliwiać automatyczne dodawanie do bazy ewidencji zasobu typu komputer, wraz z informacjami o producencie, modelu i podzespołach na podstawie danych przesłanych przez agenta. 23. Oprogramowanie musi posiadać funkcję wykrywania duplikatów komputerów. 24. Oprogramowanie musi posiadać możliwość automatycznego rozpoznania typu komputera w szczególności: laptop, desktop, serwer, wirtualna maszyna na podstawie informacji przesłanych przez agenta. 25. Oprogramowanie musi posiadać możliwość konfiguracji własnych słowników statusów i podstatusów zasobów. 26. Oprogramowanie musi umożliwiać ustawienie właściciela zasobu w przypadku przypisania wielu osób do tego samego zasobu. 27. Oprogramowanie musi umożliwiać automatyczne sugerowanie osób, które mogą być potencjalnymi użytkownikami komputera. 28. Oprogramowanie musi automatycznie tworzyć i aktualizować relację komputera z osobą zaewidencjonowaną w bazie CMDB, np. gdy łączny czas użycia komputera przez daną osobę przekracza 80% w okresie 30 dni (parametry konfigurowalne). 29. Oprogramowanie musi przysyłać cykliczne raporty o stanie komputera z zainstalowanym agentem, zgodnie z czasem skonfigurowanym w profilu agenta, w szczególności o: statusie połączenia (offline/online), liście zainstalowanego oprogramowania, danych z monitoringu, informacji o konfiguracji sprzętu, informacji o zmianach w konfiguracji sprzętu i oprogramowania, parametrów obciążenia komputera: średniej zajętość dysku twardego, średniego obciążenia procesora, średniego obciążenia pamięci RAM, top 5 procesów najbardziej obciążających CPU, top 5 procesów najbardziej obciążających pamięć RAM, top 5 procesów najbardziej obciążających sieć. 30. Oprogramowanie musi posiadać natywne konektory do systemów witalizacyjnych Microsoft Hyper-V oraz VMWare (wersja min. 6.5.) w celu automatycznego pobierania informacji o maszynach wirtualnych, włącznie z ich parametrami oraz stanem. 31. Oprogramowanie musi posiadać graficzny cykl życia dla każdego jednego zasobu, który musi zapisywać wszystkie ważne informacje związane z cyklem życia zasobu w organizacji, w szczególności: zmiany dowolnych cech zasobu w formacie "było X jest Y", zmiany w konfiguracji sprzętu np. wykryto oprogramowanie X, odinstalowano oprogramowanie Y, zmiany statusu dostępności, alerty związane ze sprzętem np. wysokie obciążenie CPU, przepełnienie dysku, wysokie obciążenie sieci, zmiana profilu agenta.
--	--

	32. Oprogramowanie musi posiadać możliwość dokonywania wpisów czynności serwisowych związanych z zasobem do historii cyklu życia zasobu np. wymiana matrycy w komputerze, wymiana tonera w drukarce itp. 33. W cyklu życia zasobów każdy wpis musi posiadać informację o dacie operacji oraz użytkowniku, który jej dokonał. 34. Cykl życia zasobów musi posiadać funkcję filtrowania oraz wyszukiwania zdarzeń w historii cyklu, wraz z możliwością wskazania zakresu dat od... do... . 35. Oprogramowanie musi umożliwiać ewidencjonowanie dokumentów faktur z możliwością dołączania skanów dokumentów. 36. Oprogramowanie musi umożliwiać prezentację danych profilu osoby zawierającego w szczególności: dane o loginie osoby oraz loginach dodatkowych, informacje o aktywności osoby na wszystkich komputerach łącznie, najczęściej użytkowanym oprogramowaniu, najczęściej odwiedzanych stronach internetowych, 37. Oprogramowanie musi umożliwiać drukowanie etykiet z kodem kreskowym lub kodem QR zawierających informacje ewidencyjne zasobów, w szczególności: logo firmy, nazwa zasobu, numer seryjny, numer ewidencyjny, kod lokalizacji, kod działu. 38. Oprogramowanie musi umożliwiać dodawanie zasobów do bazy CMDDB po kodzie SKU/EAN w szczególności: licencji, laptopów, drukarek, urządzeń sieciowych. W przypadku braku kodu SKU/EAN na produkcie, system musi umożliwiać dodanie pozycji ręcznie. 39. Oprogramowanie musi posiadać bazę słowników produktów licencyjnych zawierającą informacje o: nazwie i producencie oprogramowania, rodzaju licencji (w szczególności: OEM, BOX, OPEN, SELECT, EA, MPSA, UPG, Cloud, PKC), okresie ważności licencji (wieczysta, subskrypcja), cenie jednostkowej (jeśli producent podaje publicznie taką informację), kod SKU/EAN, prawa licencyjne (w szczególności: Direct – licencjonowanie bezpośrednie, Downgrade – pokrycie starszych wersji oprogramowania, Upgrade – możliwość aktualizacji do nowszych wersji oprogramowania, Pokrycie komponentów pakietu oprogramowania, Pokrycie maszyn wirtualnych, Upgrade pod warunkiem posiadania podstawy – innej wymaganej licencji, Software Assurance, Ograniczenie jednoczesnego użycia oprogramowania, External Connector, MSDN, Education – użycie na urządzeniach szkoleniowych, Per Site, Licencjonowanie na urządzenie, Licencjonowanie na serwer, Licencjonowanie na procesor, Licencjonowanie na rdzeń procesora, Licencjonowanie na użytkownika, Licencjonowanie na usługę, Licencjonowanie na urządzenie sieciowe). 40. Oprogramowanie musi posiadać bazę produktów handlowych dla komputerów, urządzeń mobilnych, drukarek, zasobów sieciowych i innych rozwijaną przez producenta, zawierającą m.in. kod SKU/EAN. 41. Oprogramowanie musi posiadać bazę wzorców identyfikujących oprogramowanie na komputerach. 42. Oprogramowanie musi umożliwiać dodawanie własnych produktów handlowych oraz wzorców oprogramowania. 43. Oprogramowanie musi posiadać gotowe raporty systemowe możliwe do wygenerowania w formacie PDF: karta pracownika, protokół zdawczo-odbiorczy, metryka komputera. 44. Oprogramowanie musi posiadać możliwość tworzenia profili pracy agentów, w ramach których musi być możliwość konfiguracji takich parametrów jak: czasy nawiązywania połączeń przez agenta do serwera, czasy przesyłania przez agenta danych do serwera, priorytet działania agenta, zakres monitorowania użytkownika, obciążenia, konfiguracja alertów sprzętowych, zakres blokowania nośników danych i urządzeń, częstotliwość wykonywania przyrostowych i pełnych audytów SAM, blokowanie łatwego odinstalowania agenta (również przy pomocy hasła). 45. Oprogramowanie musi posiadać możliwość ustawienia zakresu obowiązywania profilu agenta w oparciu o przypisanie komputera do działu, lokalizacji i osoby w scenariuszu, np. „ustaw profil dla komputerów w działach A i B, ale tylko jeżeli są w lokalizacji D lub E”. 46. Oprogramowanie musi umożliwiać konfigurację wielu grup akceptacyjnych i określenie nieograniczonej liczby osób wchodzących w skład grupy. 47. Oprogramowanie musi umożliwiać zdefiniowanie wymaganej, minimalnej liczby członków (kworum) grupy akceptacyjnej, która jest wymagana do uzyskania pozytywnego/negatywnego wyniku całej akceptacji
Zarządzanie zasobami oprogramowania	1. Oprogramowanie musi przy pomocy agenta zbierać dane o zainstalowanym oprogramowaniu na urządzeniach typu komputer.

	2. Oprogramowanie musi automatycznie przeprowadzać analizę identyfikacji zainstalowanego oprogramowania na podstawie bazy wzorców oprogramowania. 3. Oprogramowanie musi zapisywać każdą informację o wykryciu oprogramowania lub jego usunięciu w historii komputera, serwera oraz samego oprogramowania. Funkcja musi także działać w sytuacji, kiedy komputer jest poza siecią firmową (zapis historii offline). 4. Oprogramowanie musi automatycznie klasyfikować oprogramowanie darmowe lub płatne wymagające zakupu licencji. 5. Oprogramowanie musi automatycznie rozpoznawać sposób licencjonowania oprogramowania typu "per device" i "per user". 6. Oprogramowanie musi sygnalizować nieużywanie oprogramowania przez użytkownika, które jest zainstalowane na komputerze. 7. Oprogramowanie musi mieć możliwość ustawienia minimalnego progu użycia oprogramowania przez użytkownika np. 30 godz. w miesiącu, 5 min. w miesiącu itp. 8. Oprogramowanie musi analizować użycie oprogramowania przez użytkownika i porównywać czy dla danego oprogramowania jest spełniony parametr "minimalnego użycia oprogramowania". Jeżeli parametr nie jest spełniony oprogramowanie musi sygnalizować taki stan na ekranie. 9. Oprogramowanie musi tworzyć automatycznie bilanse stanu niezgodności licencji wraz z informacją o niskim użyciu oprogramowania. 10. Oprogramowanie musi umożliwiać automatyczne rozliczenie licencji poprzez przypisanie wolnych licencji do komputerów lub użytkowników w zależności od sposobu licencjonowania. 11. Bilans licencji utworzony w oprogramowaniu musi być podzielony na grupy oprogramowania np. oddzielnie systemy operacyjne dla komputerów, oddzielnie systemy operacyjne dla serwerów, oddzielnie oprogramowanie Office, oddzielnie oprogramowanie graficzne itd. 12. Baza wzorców oprogramowania musi posiadać uzupełnione kody SKU dla najpopularniejszych produktów licencyjnych z możliwością ich ręcznego uzupełnienia. 13. Oprogramowanie musi posiadać funkcję inteligentnego sugerowania użytkownikowi jaka licencja, którą może zakupić, pasuje do zainstalowanego oprogramowania. 14. Oprogramowanie musi automatycznie wyliczać wartość PVU dla produktów IBM'a. 15. Oprogramowanie musi automatycznie wyliczać wartość OCF dla produktów Oracle. 16. Oprogramowanie musi umożliwiać utworzenie raportu Bilansu Licencji. 17. Oprogramowanie musi umożliwiać ewidencjonowanie licencji przypisanych do urządzeń sieciowych. 18. Oprogramowanie musi zawierać bazę słowników oprogramowania zawierającą m.in. informacje o producencie; nazwie oprogramowania; wersji; typie oprogramowania; informacje o tym, czy oprogramowanie jest płatne dla firm; rodzaju instalacji (on-premise, public (SaaS), portable, sieć), wzorcu generycznym zawierającym rozbudowane składnie zapytań do plików, rejestrów danych z monitoringu aplikacji i stron www. 19. Oprogramowanie musi posiadać możliwość tworzenia własnych słowników i wzorców oprogramowania.
Automatyzacja	1. Oprogramowanie musi umożliwiać tworzenia reguł automatyzujących pracę oprogramowania w oparciu o warunki, wyzwalacze i akcje wykonawcze, zgodnie z zasadą "if THIS then THAT". 2. Oprogramowanie musi umożliwiać stworzenie reguły automatycznej zmiany status zasobu w chwili przekroczenia wybranej daty np. terminu gwarancji zasobu, daty końca wsparcia przez producenta czy daty planowanej wymiany. 3. Oprogramowanie musi umożliwiać stworzenie reguły wysyłania dowolnego raportu z hurtowni danych do wybranych osób lub działów w zadanym cyklicznym harmonogramie czasowym. 4. Oprogramowanie musi umożliwiać stworzenie reguły ustawiającej wartość dla wybranego pola z możliwością ustawienia także funkcji autonumerowania pola wg wskazanego licznika. Funkcja musi posiadać możliwość określenia innych wartości dla różnych lokalizacji zasobów. 5. Oprogramowanie musi umożliwiać stworzenie reguły automatycznie zmieniającej status zasobu w chwili łączenia dwóch zasobów relacją w szczególności np. gdy

	przypisywany jest użytkownik do komputera, który ma status "w magazynie" ma stworzyć relację komputer-osoba i automatycznie ustawić status komputera na "w użyciu". 6. Oprogramowanie musi umożliwiać stworzenie reguły automatycznie zmieniającej status zasobu w chwili odłączania relacji od zasobu w szczególności np. gdy odłączyć użytkownika od komputera, wówczas status komputera musi zmienić się na "w magazynie".
Sieć	1. Oprogramowanie musi posiadać mechanizmy umożliwiające skanowanie całej sieci wraz z podsieciami przy pomocy skanerów sieci z zastrzeżeniem, że każda podsieć musi być skanowana przy pomocy oddzielnego skanera, skonfigurowanego dla danej podsieci i zainstalowanego w danej podsieci. 2. Oprogramowanie musi umożliwiać uruchomienie 1 skanera sieci. 3. Oprogramowanie musi umożliwiać konfigurację wielu zakresów adresów IP wraz z możliwością pomijania wybranych zakresów adresacji IP. 4. Oprogramowanie musi umożliwiać prezentację listy wszystkich sieci oraz podsieci. 5. Oprogramowanie musi umożliwiać definiowanie sieci nadrzędnej. 6. Oprogramowanie musi umożliwiać definiowanie i skanowanie portów na adresach IP w celu monitorowania działania usług sieciowych. 7. Oprogramowanie musi umożliwiać automatyczne i ręczne wiązanie relacją wykrytych w sieci urządzeń z zasobami zaewidencjonowanymi w oprogramowaniu. 8. Oprogramowanie musi automatycznie wykrywać nowe urządzenia w sieci wraz z możliwością powiadomienia wskazanych osób o wykryciu nowego urządzenia w danej sieci. 9. Oprogramowanie musi automatycznie zmieniać status dostępności zasobu na "nieдоступny", w chwili, kiedy urządzenie nie zwraca pozytywnego wyniku skanowania i zmieniać status dostępności zasobu na "dostępny", w chwili, kiedy urządzenie zwraca pozytywny wynik skanowania. 10. Oprogramowanie musi rejestrować datę ostatniej aktywności, czas nieprzerwanej aktywności oraz czas przestoju.
Helpdesk	1. Oprogramowanie musi zapewniać możliwość założenia prostego zadania przez każdego użytkownika przy pomocy formularza lub poprzez wysłanie wiadomości e-mail na skonfigurowaną skrzynkę pocztową. 2. Zadanie musi posiadać możliwość określenia jego tytułu, opisu, początku i końca realizacji, czasochłonności, priorytetu, kategoryzacji oraz musi mieć możliwość wskazania innego wykonawcy niż twórca. 3. Oprogramowanie w zakresie funkcji zadań musi także umożliwiać prowadzenie rozmów w formie czatu lub zapisywania notatek w tym także załączania dowolnych załączników. 4. Zadanie musi posiadać wbudowany proces umożliwiający realizację zadania w krokach: nowe, otwarte, w realizacji, wstrzymane, zamknięte. 5. Oprogramowanie musi posiadać cykl życia zadania zapisujący i prezentujący wszystkie akcje wykonane w zadaniu m.in. zmiany wartości pól, zmiany etapów zadania. 6. Oprogramowanie musi posiadać funkcjonalność utworzenia zadania o typie decyzja, które musi posiadać przepływ zapewniający realizację zadania w krokach: oczekiwanie na decyzję, akceptacja, odrzucenie oraz brak decyzji. Pozostałe funkcje zadania typu decyzja muszą być tożsame z funkcjami zadania. 7. Oprogramowanie musi posiadać podręczną listę zadań, dostępną z każdego miejsca oprogramowania z funkcją sortowania, filtrowania i wyszukiwania zadań. 8. Oprogramowanie musi posiadać graficzny widok kalendarza, prezentujący zaplanowane i zrealizowane zadania w widoku dziennym, tygodniowym i miesięcznym. 9. Widok kalendarza musi zapewniać możliwość zaprezentowania kalendarza zadań dla dowolnej wybranej osoby, jeżeli osoba zalogowana posiada stosowne uprawnienia np. Szef działu może zobaczyć kalendarze swoich pracowników. 10. Funkcja kalendarza musi zapewniać możliwość zmiany terminu realizacji zadania za pomocą funkcji drag&drop. 11. Funkcja kalendarza musi posiadać możliwość utworzenia zdarzenia pojedynczego lub cyklicznego w kalendarzu wraz z możliwością określenia kategorii tego zdarzenia. Zdarzenie cykliczne jest rozumiane jako czynność powtarzająca się lub może pełnić funkcję blokowania terminów, aby inni współpracownicy widzieli plan pracy danej osoby. 12. Oprogramowanie musi ofertować oddzielną witrynę dla pracowników firmy, osób współpracujących, kontrahentów itp. służącą do składania anonimowych wniosków (obsługa Sygnalistów) bez konieczności logowania się i pozostawiania jakichkolwiek danych osobowych.

	13. Oprogramowanie musi zapewniać Sygnaliście także możliwość weryfikacji statusu sprawy oraz korespondowania w jej zakresie poprzez użycie wygenerowanego podczas składania wniosku jednorazowego tokenu. 14. Oprogramowanie musi powiadamiać przy pomocy mail użytkownika o zmianach w jego zadaniu, o zbliżającym się terminie lub jego upływie.
Monitorowanie	1. Oprogramowanie musi umożliwiać monitoring aktywności komputerów, serwerów i maszyn wirtualnych z systemami Windows. 2. Oprogramowanie musi monitorować logowania użytkowników ze wskazaniem loginu użytkownika, nazwy komputera, rodzaju akcji. 3. Oprogramowanie musi monitorować użycie oprogramowania ze wskazaniem nazwy i wersji oprogramowania, loginu użytkownika, nazwy komputera, łącznego czasu użycia, udziału procentowego użycia. 4. Oprogramowanie musi monitorować odwiedziny stron internetowych ze wskazaniem domeny, loginu użytkownika, nazwy komputera, łącznego czasu odwiedzin, udziału procentowego odwiedzin. 5. Oprogramowanie musi monitorować operacje na plikach ze wskazaniem nazwy użytkownika, nazwy komputera rodzaju akcji, rodzaju nośnika. 6. Oprogramowanie musi monitorować wydruki ze wskazaniem loginu użytkownika, nazwy komputera, nazwy drukarki, liczby dokumentów, liczby stron. 7. Oprogramowanie musi umożliwiać prezentację danych o okresach 30, 90 i 180 dni.
Zarządzanie urządzeniami	1. Oprogramowanie musi automatycznie tworzyć zasób typu nośnik danych w chwili podłączenia takiego nośnika do komputera z agentem. 2. Oprogramowanie musi umożliwiać blokowanie użycia nośników danych: dysków zewnętrznych i pendrive'ów, czytników kart pamięci, nośników optycznych, nośników bluetooth, modemów mobilnych i drukarek. 3. Oprogramowanie musi posiadać rejestr połączeń i rozłączeń nośników zawierający: nazwę komputera, na którym użyto nośnika, nazwę konta użytkownika, który użył nośnika, identyfikator nośnika i datę podłączenia/rozłączenia. 4. Oprogramowanie musi umożliwiać autoryzację wybranych nośników USB lub czytników kart pamięci, aby były dozwolone do użycia pomimo blokady nośników. 5. Oprogramowanie musi umożliwiać automatyczne tworzenie zasobu w momencie podłączenia nośnika danych do komputera z zainstalowanym agentem. 6. Oprogramowanie musi umożliwiać rejestrowanie zdarzeń podłączenia, rozłączenia i zablokowania nośnika w cyklu życia komputera oraz nośnika danych.
Skrypty	1. Oprogramowanie musi posiadać wbudowany edytor skryptów z funkcją podświetlania składni, służący do tworzenia dowolnych skryptów Batch i PowerShell. 2. Oprogramowanie musi umożliwiać wywoływanie utworzonych skryptów na komputerach oraz grupach komputerów z zainstalowanym agentem. 3. Oprogramowanie musi posiadać funkcję zwracania do serwera informacji o statusie wykonania skryptu, a w przypadku niepowodzenia działania skryptu, przekazanie do serwera informacji o kodzie błędu i całej linii komunikatu błędu. 4. Oprogramowanie musi umożliwiać przechowywanie pełnej historii użycia skryptów oraz wyników ich wykonania na poszczególnych komputerach. 5. Oprogramowanie musi umożliwiać tworzenie repozytorium dowolnych plików i automatycznej ich dystrybucji na komputery z zainstalowanym agentem. 6. Oprogramowanie musi umożliwiać wykonanie cichej instalacji i dezinstalacji oprogramowania z pakietów msi i exe (przy założeniu, że instalator danego oprogramowania zezwala na cichą instalację, na wybranych grupach komputerów).
Zdalny dostęp	1. Oprogramowanie musi umożliwiać zdalne połączenie w trybie view-only i w trybie pełnego przejęcia pulpitu komputera bezpośrednio z poziomu przeglądarki internetowej, bez instalacji dodatkowego oprogramowania na urządzeniu, z którego jest nawiązywane połączenie. 2. Oprogramowanie musi umożliwiać połączenie z dowolnym komputerem z zainstalowanym agentem, niezależnie od adresu IP nadanego dla danego komputera, a także gdy komputer znajduje się w sieci Internet, za NAT. 3. Oprogramowanie musi umożliwiać nawiązanie wielu sesji w tym samym czasie z różnymi komputerami. 4. Oprogramowanie musi rejestrować historię nawiązanych połączeń. 5. Oprogramowanie musi umożliwiać transfer dowolnych plików do komputera w trakcie trwania sesji zdalnego pulpitu i zapisywanie tych zdarzeń w historii.

	6. Oprogramowanie musi umożliwiać konfigurację zdalnego połączenia, aby wymagało potwierdzenia przez użytkownika końcowego. 7. Oprogramowanie musi umożliwiać wywołanie komunikatu informującego o połączeniu na ekranie użytkownika końcowego.
Wymagania dodatkowe	1. Interfejs użytkownika dostępny w języku polskim i angielskim. 2. Oprogramowanie musi posiadać dokumentację użytkownika i administratora w polskiej wersji językowej dostępną online. 3. Wyświetlanie wraz z ładowaniem danych na ekranie użytkownika musi się odbywać w czasie nieprzekraczającym 3 sekundy w szczególności dla ekranów (ekrany podsumowania, ekrany z tabelami danych, ekrany szczegółów zasobów w tym okien edycji). 4. Oprogramowanie musi posiadać architekturę typu Klient-Serwer z dostępem dla użytkownika poprzez przeglądarkę internetową, w szczególności EDGE, Chrome, Firefox, Opera, Safari (wersja przeglądarki nie starsza niż 12 miesięcy). 5. Oprogramowanie musi umożliwiać równoległą pracę dla użytkowników, z poziomu komputera, tabletu oraz smartphona, w ilości minimum 34. 6. Oprogramowanie musi umożliwiać instalację Serwera Aplikacji na środowisku wirtualnym na systemie operacyjnym Linux oraz Windows Server 2008 R2 i wyższej. 7. Oprogramowanie musi umożliwiać instalację agentów na komputerach z systemem Windows 7 i wyższej w ilości minimum 34. 8. Dostarczona licencja na oprogramowanie musi być wieczysta. 9. Oprogramowanie musi zapewniać obsługę w sieci WLAN, bezprzewodowych sieci lokalnych. 10. Oprogramowanie musi być wyposażone w mechanizm integracji metodą REST-API. 11. Oprogramowanie musi posiadać w pełni udokumentowane metody REST-API m.in GET/PUT/POST. 12. Oprogramowanie musi współpracować z silnikami bazodanowymi Microsoft SQL oraz PostgreSQL. 13. Aktualizacja Oprogramowania musi się odbywać bez konieczności logowania się do systemu operacyjnego, na którym działa Serwer Aplikacji (przez przeglądarkę). 14. Oprogramowanie musi umożliwiać przeglądanie danych zgodnie z metodą "od ogółu do szczegółu" (drill-down). 15. Oprogramowanie musi zapewniać szyfrowaną komunikację pomiędzy każdym elementem systemu. Kanał transportowy (TCP) pomiędzy agentami, a serwerem szyfrowany algorytmem AES (Rijndael). Klucz zdefiniowany w konfiguracji serwera. Informacje przesyłane między klientem (aplikacja web), a serwerem muszą być zabezpieczone protokołem TLS. 16. Oprogramowanie musi działać w sieciach o adresacji IPv4 i IPv6. 17. Oprogramowanie musi posiadać mechanizm rejestrowania i logowania błędów. 18. Oprogramowanie musi posiadać bazę produktów handlowych aktualizowaną regularnie przez producenta. Baza musi zawierać co najmniej 1 milion pozycji obejmującą co najmniej komputery, laptopy, smartphony, drukarki, licencje, oprogramowanie, routery. 19. Oprogramowanie musi wspierać realizację dobrych praktyk w zarządzaniu IT w oparciu o biblioteki ITIL.
Wsparcie wdrożeniowe	W ramach dostawy Zamawiający wymaga, aby została udzielona asysta techniczna przy uruchomieniu systemu i przeprowadzeniu podstawowego przeszkolenia administratora systemu i wsparciem przy wdrożeniu w zakresie minimum 6 godzin roboczych, w formie zdalnej.

Certyfikowane szkolenie dla administratora z dostarczonego urządzenia klasy UTM

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenie stacjonarne dla administratora z zakresu dostarczonego urządzenia klasy UTM wraz z egzaminem
Program szkolenia	1. Praca z urządzeniem

	• Rejestracja w strefie klienta i dostęp zasobów • Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego • Ustawienia systemowe i uprawnienia administratorów • Instalacja licencji i aktualizacja systemu • Tworzenie kopii zapasowej i przywracanie konfiguracji 2. Zbieranie logów i monitorowanie • Przedstawienie kategorii zbieranych logów • Wykresy historyczne i monitorowanie 3. Obiekty • Typy obiektów oraz ich wykorzystanie • Obiekty sieciowe i obiekt typu „router” 4. Konfiguracja sieci • Tryby pracy urządzenia • Typy interfejsów (Ethernet, modem, bridge, VLAN, GRE/TAP) • Typy routingu oraz ich priorytety 5. Translacja adresów sieciowych (NAT) 6. Translacja połączeń wychodzących (maskarada) 7. Translacja połączeń przychodzących (przekierowanie) 8. Translacja dwukierunkowa (jeden do jeden) 9. Filtrowanie ruchu sieciowego (Firewall) 10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection) • Szczegółowy opis parametrów reguły Firewall • Kolejność przetwarzania reguł Firewall i NAT 11. Ochrona aplikacji • Implementacja filtrowania URL dla ruchu http i https • Konfigurowanie skanowania antywirusowego i modułu Breach Fighter • Moduł IPS i stosowanie profili inspekcji 12. Użytkownicy i uwierzytelnianie 13. Konfiguracja usługi katalogowej • Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO) • Rejestracja użytkowników • Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania 14. Wirtualne sieci prywatne (VPN) • Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2) • Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK) • Tunele VTI 15. SSL VPN • Zasada działania • Konfiguracja
Wymagania dodatkowe	W ramach realizacji szkolenia wymagane jest, aby: - Szkolenie zdalne, realizowane przez autoryzowane centrum szkoleniowe przez producenta dostarczonego urządzenia klasy UTM - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych, - Uczestnik po zakończeniu szkolenia musi otrzymać zaświadczenie ukończenia szkolenia - Uczestnik musi mieć możliwość bezpłatnego 14-sto dniowego kontaktu z trenerem po szkoleniu.
Ilość	Szkolenie dla 1 administratora

Wymagania dodatkowe

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostawy przedmiotu zamówienia wraz z jego rozpakowaniem, sprawdzeniem poprawności działania i ustawieniem w wyznaczonym przez Zamawiającego pomieszczeniu na terenie Urzędu.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Wykonawca zobowiązany do utylizacji na własny koszt wszelkich niepotrzebnych materiałów zabezpieczających urządzenia podczas transportu, w tym kartony, folie, taśmy klejące etc.

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.