numer sprawy: CG.ZP.D.272.54.2021.AS
załącznik nr 2 do specyfikacji warunków zamówienia (SWZ)

Spis treści

1. Dostawa infrastruktury, tym Sprzętu, Oprogramowania oraz kabli światłowodowych

Wykonawca dostarczy, zainstaluje i skonfiguruje infrastrukturę teleinformatyczną składającą się z następujących elementów:

1.1 Przełącznik rdzeniowy - 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Wysokość w szafie 19” – 1U. Głębokość nie większa niż 53cm
Wyposażenie	- Minimum 48 portów 10GbE/25GbE SFP28 umieszczonych z przodu obudowy (z czego min. 35 portów wyposażonych we wkładki światłowodowe SFP+ 10G-Base-LR w pełni kompatybilne z dostarczanym przełącznikiem). Wszystkie porty muszą być aktywne - Minimum 8 portów 40GbE/100GbE QSFP28 umieszczonych z przodu obudowy (min. 2 porty wyposażone we wkładki 100G QSFP28 LR4 w pełni kompatybilne z dostarczanym przełącznikiem, min. 2 porty wyposażone w kable DAC 100G QSFP28 w pełni kompatybilne z dostarczanym przełącznikiem). Wszystkie porty muszą być aktywne - Wbudowany, dodatkowy, dedykowany port Ethernet SFP do zarządzania poza pasmem - out of band management - Port konsoli RS232 ze złączem DB9 lub RJ45 - Port USB 2.0 (niezależny od portu konsoli) - Wielkość bufora pakietów (packet buffer): minimum 16MB - Pamięć RAM: co najmniej 8GB - Pamięć nieulotna typu flash (zabudowana, nie dopuszcza się pamięci zewnętrznej typu pendrive, itp.): co najmniej 1GB - Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) - Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. - Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
Parametry wydajnościowe	- Wydajność: minimum 4 Tb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) - Przepustowość: minimum 2000 Mp/s
Funkcjonalność	- Przełączanie w warstwie 2 i 3 modelu OSI - Opóźnienie przełączania transmisji 10GbE dla pakietów 64 bajtowych poniżej 1µs - Mechanizmy przełączania: co najmniej cut through - Wielkość tablicy routingu: minimum 320000 wpisów dla IPv4 oraz min. 160000 dla IPv6 - Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie. Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 480 portów 25GbE SFP28. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)). **Przełączniki muszą łączyć się we wspólne stosy z posiadanymi przez Partnera Projektu przełącznikami serii HPE 5945.** - Łącznie w stos z wykorzystaniem portów 25GbE, 40GbE, 100GbE i agregowanych portów 25GbE, 40GbE, 100GbE (w celu zwiększenia przepustowości w stosie) - Możliwość realizacji łączy agregowanych w ramach różnych przełączników będących w stosie - Możliwość realizacji łączy agregowanych w ramach różnych przełączników nie będących w stosie (tzw. MLAG, Multi chassis Link Aggregation) - Tablica adresów MAC o wielkości minimum 280000 pozycji - Tablica ARP o wielkości minimum 64000 wpisów - Obsługa ramek Jumbo o wielkości minimum 9400B - Obsługa Quality of Service - Obsługa mechanizmów: strict priority (SP) queuing, weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR), explicit congestion notification (ECN) oraz SP+WDRR - Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) - Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ - Obsługa IGMP v1/v2/v3 oraz IGMP Snooping - Obsługa MLD v1/v2 oraz MLD Snooping - Wsparcie dla FibreChannel over Ethernet - Obsługa VXLAN

	- Wsparcie dla Data Center Bridging (DCB): • Data Center Bridging Exchange (DCBX) • IEEE 802.1Qbb Priority Flow Control (PFC) • IEEE 802.1Qaz Enhanced Transmission Selection (ETS) - Routing IPv4 – statyczny i dynamiczny (min. RIP, OSFP, ISIS, BGP) - Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSPFv3, IS-ISv6, BGP4) - Obsługa Policy Based Routing (dla IPv4 i IPv6) - Obsługa PIM-DM, PIM-SM, PIM-SSM oraz BIDIR-PIM - Obsługa Multicast Source Discovery Protocol (MSDP) - Obsługa Multicast VLAN - Obsługa tunelowania GRE - Funkcja mapowania VLAN - Obsługa mechanizmów: Dual stack (RFC 2893), Tunneling (RFC 2893) oraz IPv6 on the provider edge routers (6PE) - Obsługa ECMP (Equal Cost Multi Path) - Obsługa mechanizmu Bidirectional Forwarding Detection (BFD) dla OSFP, ISIS, BGP, OSPFv3, IS-ISv6, BGP4+, PIM oraz routing statycznego - Obsługa Virtual Router Redundancy Protocol (VRRP) - Funkcja pozwalająca na automatyczne wyłączenie określonego połączenia w przypadku awarii innego, określonego połączenia - Obsługa Ethernet Ring Protection Switching (ERPS) - Funkcja izolacji portów - Serwer DHCP (RFC 2131), klient DHCP, obsługa opcji 82 (RFC 3046), DHCP snooping, serwer DHCPv6 - Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia - Obsługa standardu 802.1p, 8 kolejek wyjściowych na każdym porcie - Funkcja ograniczania pasma na porcie - Funkcja zmiany wartości pola DSCP i wartości priorytetu 802.1p - Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, Flow mirroring, L2 remote mirroring - Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS - Zarządzanie poprzez port konsoli, SNMP v1, 2c i 3, Telnet, SSH v2 - Obsługa Syslog - Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED - Obsługa sFlow - Obsługa Network Configuration Protocol (NETCONF) - Obsługa Network Time Protocol (NTP) i Simple Network Time Protocol (SNTP) - Obsługa Ethernet OAM - Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego - Modularny system operacyjny ze wsparciem dla In Services Software Upgrade (ISSU) i skryptów w języku Python oraz TCL - Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter - Funkcja przechwytywania pakietów (packet capture) i zapisywania ich do pliku typu pcap z możliwością późniejszej ich analizy przy pomocy zewnętrznego oprogramowania oraz bezpośrednio na przełączniku -Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 - Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). - Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

	- Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. - Maksymalny pobór mocy nie większy niż 700W
Inne	Jeżeli uruchomienie którejkolwiek z ww. funkcjonalności wymaga dodatkowej licencji, Wykonawca zobowiązany jest do jest dostarczenia. Licencje muszą być permanentne, nie dopuszcza się licencji czasowych.
Gwarancja	Minimum 5 letni serwis producenta obejmujący wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający reakcję w miejscu instalacji maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania urządzenia oraz wsparcia technicznego z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu z oprogramowaniem. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Partnerem Projektu i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego.

Zamawiający posiada 2 sztuki urządzenia HPE 5945 Series Switch wraz z wyposażeniem (48 wkładek światłowodowych 10G-baseLR, 2 kable DAC 100G). Zamawiający dopuszcza wymianę istniejących urządzeń pod warunkiem dostarczenia urządzeń o parametrach nie gorszych od urządzeń opisanych w tabeli powyżej i nie gorszych od urządzeń posiadanych przez Partnera Projektu. W przypadku wymiany łączna ilość dostarczanych urządzeń to 4 sztuki.

1.2 Przełącznik dostępowy - 24 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	• Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 40cm.
Wyposażenie	• Co najmniej 48 porty GE w standardzie 10/100/1000BaseT wspierających standard 802.3at (PoE+) • Minimum 4 porty 10Gigabitowe SFP+, niezależne od wymaganych portów 10/100/1000BaseT (z czego min. 2 porty obsadzone wkładkami 10GBase-LR w pełni kompatybilnymi z dostarczanymi przełącznikami). Wszystkie porty muszą być aktywne
Funkcjonalność	• Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 100/1000BaseX i ich kombinacji • Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie • Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP • Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng • Policy Based Routing • Wsparcie dla Bidirectional Forwarding Detection (BFD) • Minimum 32 interfejsy IP VLAN • Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping

	• Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol • Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN • Obsługa IEEE 802.1ad QinQ i Selective QinQ • Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree • BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom • Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) • Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI • Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia • Obsługa standardu 802.1p – min. 8 kolejek na porcie • Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p • Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP • Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring • Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x: • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników • LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED • Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC • TACACS+ i RADIUS Network Login • RADIUS Accounting • Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS • Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https • Syslog • Obsługa NETCONF • Obsługa sFlow • Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3 • Obsługa NTP i SNTP • Obsługa protokołów 802.3ah oraz 802.1ag • Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu • sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter • Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego • Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol • Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych • **Przełączniki muszą łączyć się we wspólne stosy z posiadanymi przez Partnera Projektu przełącznikami serii HPE 5130 EI**
Gwarancja	Minimum 5 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego (niezależnego od

	zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Partner Projektu musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
Inne	• Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji producenta. • Wszystkie przełączniki muszą być fabrycznie nowe. • Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT • Wydajność przełączania co najmniej 170 Gbps oraz przepustowość min. 130 Mpps • Minimalny zakres pracy od -5°C do 45°C • Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. • Minimum 512MB Flash • Minumim 1GB RAM • Bufor pakietów nie mniejszy niż 3MB • Budżet mocy dla PoE: min. 370W • Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3 • Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). • Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). • Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

Partner Projektu posiada:

- 8 sztuk urządzenia HPE FlexNetwork 5130 48G PoE+ 4SFP+ (370W) EI Switch wraz z 2 wkładkami 10Gbase-LR

- 1 sztukę urządzenia HPE FlexNetwork 5130 24G PoE+ 4SFP+ (370W) EI Switch wraz z 2 wkładkami 10Gbase-LR

Zamawiający dopuszcza wymianę istniejących urządzeń pod warunkiem dostarczenia urządzeń o parametrach nie gorszych od urządzeń opisanych w tabeli powyżej i nie gorszych od urządzeń posiadanych przez Partnera Projektu. W przypadku wymiany łącza ilość dostarczanych urządzeń to 33 sztuki.

1.3 Urządzenie Firewall - 1 kpl.

Wymagania ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje.

Dostarczony system powinien pracować w trybie wysokiej dostępności (HA Active-Pasive oraz HA Active-Active). **Dostarczone urządzenie powinno dawać możliwość połączenia w klaster HA z urządzeniem Fortigate 100F będącym w posiadaniu Partnera Projektu**. Partner Projektu posiada urządzenie Fortigate 100F (numer seryjny jest tajemnicą

przedsiębiorstwa i zostanie przekazany Wykonawcy po podpisaniu Umowy) z gwarancją i wsparciem producenta do dnia 13 stycznia 2024 roku . Zamawiający wymaga zrównania gwarancji, wsparcia producenta, subskrypcji obecnie posiadanego urządzenia oraz nowego urządzenia dostarczanego w ramach klastra HA.

Zamawiający dopuszcza wymianę posiadanego urządzenia Fortigate 100F pod warunkiem dostarczenia rozwiązania zapewniającego funkcjonalnie i wydajnościowo parametry nie gorsze niż opisane w tabeli poniżej i parametry nie gorsze od posiadanego przez Partnera Projektu urządzenia. W przypadku wymamiany wymagane jest dostarczenie min. dwóch urządzeń pracujących w trybie HA.

Dostarczony system bezpieczeństwa musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Możliwość filtrowania URL.
4. Inspekcję ruchu szyfrowanego https.
5. Ochronę przed niechcianą pocztą (AntySPAM).
6. Rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.
7. Filtrowanie treści w oparciu o typy MIME.
8. Mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.

Parametry minimalne pojedynczego urządzenia:

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Podstawowe funkcjonalności	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q
Wyposażenie	System realizujący funkcję Firewall powinien dysponować: - minimum 10 portami Ethernet 10/100/1000 Base-TX - minimum 8 portami SFP 10/100/1000 Base-X (z czego maksymalnie 4 mogą być współdzielone z portami 1G 10/100/1000 Base-TX) - minimum 2 porty SFP+ - minimum 1 port konsolowy (RS-232 w postaci złącza USB lub RJ-45) -minimum dwa redundantne zasilacze

Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 55 tys. nowych połączeń na sekundę Przepustowość Firewall'a: nie mniej niż 19 Gbps. dla pakietów 1518 Bajtów oraz min. 17.5 Gbps dla pakietów 512 Bajtów Wydajność szyfrowania VPN IPSec: nie mniej niż 11.4 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1,55 Gbps. Wydajność skanowania ruchu z włączonymi funkcjami: Firewall, IPS, AC - minimum 780 Mbps.
Logowanie i korelacja zdarzeń	System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze. System powinien mieć możliwość logowania do dedykowanego, centralnego systemu logowania producenta.
Kontrola Malware	System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.

Funkcje UTM/NGF	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection b) Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN d) Ochrona przed atakami - Intrusion Prevention System e) Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM f) Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP g) Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma h) Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) i) Możliwość analizy ruchu szyfrowanego protokołem SSL j) Mechanizmy ochrony przed wyciekiem poufnej informacji
IPSec VPN	W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: a) Tworzenie połączeń w topologii Site-to-site oraz Client-to-site b) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności c) Praca w topologii Hub and Spoke oraz Mesh d) Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF e) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
Klient VPN	W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
Routing i NAT	Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Translacja adresów NAT adresu źródłowego i docelowego.
Oddzielne instancje	Możliwość budowy minimum 8 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
Firewall	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
Antyvirus	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
IPS	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 2000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

Application Control	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
Filtr treści WWW	Baza filtra WWW o wielkości co najmniej milion adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
Filtr URL	Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
Obsługa użytkowników i integracja z zewnętrznymi bazami danych	System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż: a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP c) haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych d) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub EAL4 dla funkcji Firewall • ICSA lub NSS Labs dla funkcji IPS • ICSA dla funkcji: SSL VPN, IPSec VPN
Zarządzanie	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Support i gwarancja	Serwisy i licencje: W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 60 miesięcy. Gwarancja na sprzęt min. 60miesięcy NBD
ISO	Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący urządzenie powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Oferent powinien przedłożyć certyfikat ISO 9001 podmiotu serwisującego.
Inne	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

1.4 Oprogramowanie do zarządzania infrastrukturą - 1kpl.

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Funkcjonalność	1. System musi być zbudowany w architekturze klient – serwer 2. Licencja na system powinna umożliwiać zarządzanie minimum 100 urządzeniami sieciowymi różnych producentów z możliwością rozbudowy do przynajmniej 5000 urządzeń sieciowych. 3. System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych w celu uzyskania redundancji. System dostarczony musi być systemem redundantnym możliwym do zainstalowania na minimum 2 serwerach 4. System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułów dających dodatkową funkcjonalność, minimalnie: a. Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA b. Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetFlow (lub podobnych protokołów) oraz analizy zawartości pakietów SMTP, FTP, http c. Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS d. Zarządzanie dostępem zdalnym Ipsec/VPN e. Wbudowany serwer TACACS f. Funkcja monitorowania wydajności aplikacji 5. System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru Systemu 6. Licencja na System musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi różnych producentów 7. System musi posiadać funkcje umożliwiać automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet 8. Zarządzanie siecią bezprzewodową WLAN złożoną z co najmniej 100 punktów dostępowych (licencja na obsługę punktów dostępowych powinna być niezależna od ogólnej licencji na urządzenia sieciowe, jeżeli punkty dostępowe używają tej samej puli licencji co inne urządzenia, sumaryczna liczba dostępnych licencji musi być odpowiednio zwiększona) 9. Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników, wsparcie dla co najmniej 5 równoczesnych sond 10. System musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP i wyświetlania informacji co najmniej o: a. Średnim wykorzystaniu CPU i pamięci RAM b. Średnim czasie odpowiedzi urządzenia c. Obciążeniu interfejsów (dla ruchu wchodzącego i wychodzącego) d. Ilość błędnych lub odrzuconych pakietów na interfejsie 11. System musi posiadać funkcje konfiguracji urządzeń po protokole SNMP i SSH 12. System musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backup'ów (ręcznie oraz automatycznie w określonych odstępach czasu) oraz grupowego implementowania konfiguracji na zarządzane urządzenia. System musi zachowywać historię tworzenia backup'ów (minimum 30 dni) wraz z informacją czy przebiegł on pomyślnie, a w przypadku, jeżeli nie, powinien także poinformować o przyczynie niepowodzenia 13. System musi pozwalać na tworzenie szablonów konfiguracji co najmniej w oparciu o cały plik konfiguracyjny, fragment konfiguracji, skrypt CLI, skrypt TCL. 14. System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń, w tym możliwość przechowywania kilku wersji oprogramowania dla jednego modelu urządzenia, możliwość importowania

	obrazu z komputera do Systemu (tzw. Offline), możliwość pobrania obrazu do Systemu bezpośrednio z Internetu (tzw. Online/LiveUpdate) 15. System musi pozwalać na globalne zarządzanie VLAN, tzn. na tworzenie, modyfikowanie oraz usuwanie VLAN jednocześnie ze wszystkich lub wybranych przełączników zarządzanych przez System. Musi istnieć także możliwość automatycznego generowania map logicznej topologii sieci obrazującej konkretny VLAN a zarządzanych urządzeniach. 16. System musi posiadać funkcję zarządzania listami kontroli dostępu (ACL), w tym: możliwość importowania ACL z urządzeń i tworzenie na ich podstawie szablonu, tworzenie ACL w systemie zarządzania, możliwość pojedynczej lub grupowej implementacji przechowywanych w systemie ACL na urządzeniach 17. System musi posiadać możliwość wyświetlania zbiorczej tablicy routingu zbudowanej w oparciu o tablice zarządzanych urządzeń 18. System musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. Dashboard (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy) 19. System musi generować alarmy na podstawie takich parametrów jak: wykorzystanie CPU, wykorzystanie RAM, temperatura urządzenia, obciążenie interfejsów fizycznych na wejściu i wyjściu, ilość odrzuconych pakietów; Muszą być dostępne co najmniej dwa poziomy alarmu dla pojedynczego parametru oraz muszą być one możliwe do zmiany. 20. System musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS'em wraz z możliwością konfiguracji konkretnego zakresu czasowego i dnia tygodnia, w którym wiadomości będą wysyłane. 21. System musi pozwalać na budowanie widoków przez administratora 22. System musi posiadać funkcje generowania raportów (co najmniej w formatach PDF, CSV, Excel, XLSX, Docx) w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta. Generowanie raportów musi się odbywać na życzenie (on demand) i w regularnych odstępach czasowych (scheduled, np. codziennie, raz w tygodniu, raz na kwartał itp.) 23. System musi posiadać narzędzia graficznej prezentacji topologii sieciowej wraz z dynamiczną prezentacją zmian stanu urządzeń oraz poziomem występujących na nich alarmów. Musi być też możliwość zmiany ikony reprezentującej urządzenie na topologii sieci wraz z możliwością wykorzystania różnych ikon dla różnych poziomów alarmów na urządzeniu. 24. System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji sprzętu używanego w sieci. 25. System musi posiadać funkcje lokalizowania użytkowników przewodowych po adresie IP lub MAC. Wynikiem musi być wskazanie konkretnego portu zarządzanego urządzenia sieciowego, do którego podłączony jest użytkownik 26. System musi posiadać funkcję powiązywania konkretnego interfejsu fizycznego zarządzanego urządzenia z adresem MAC urządzenia końcowego, które będzie miało dostęp do sieci tylko na tym interfejsie. Po wykryciu nieautoryzowanej próby połączenia musi być możliwość wygenerowania alarmu, wyłączenia interfejsu po określonym czasie od zaistnienia zdarzenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) oraz ponownego włączenia interfejsu po określonym czasie od wyłączenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) 27. System musi posiadać predefiniowaną bazę zakresów adresów MAC dla urządzeń sieciowych oraz biurowych wiodących producentów. Baza musi być zbudowana co najmniej dla takich producentów jak: Cisco, Epson, Toshiba, NEC, Nortel, Canon, Sony, Samsung, 3Com, Siemens, Nokia, Apple, Lexmark, Xerox, Avaya, D-Link, LG, Dell, Alcatel, Netgear, HPE, TP-Link, Ruckus oraz Huawei. Musi istnieć możliwość ręcznego dodania wpisu do tej bazy. 28. System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie 29. System musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym, w tym: a. Wykrywanie ataków między innymi takich jak: Duplicate ARP Address, ICMP Flood, TCP Port Scan, WinNuke, IP Spoofing, ICMP Redirect,

Source Route, SYN Flood, UDP Port Scan, UDP Flood, Ping of Death, DHCP Server Detect

b. Stworzenie topologii obrazującej logiczne połączenia między urządzeniami objętymi jednym lub kilkoma atakami sieciowymi, tzn. pokazuje urządzenie/urządzenia będące źródłem ataku i łączy je z urządzeniem/urządzeniami będącymi celem ataku.

c. Stworzenie topologii obrazującej fizyczne połączenie między urządzeniami objętymi pojedynczym atakiem sieciowym, tzn. pokazuje całą ścieżkę fizyczną między źródłem, a celem ataku.

30. System musi posiadać funkcję Telnet/SSH oraz GUI proxy umożliwiającą zarządzanie CLI/Web przez przeglądarkę Internetową
31. System musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android
32. System musi posiada funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox)
33. System musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail
34. System musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń. Dodatkowo musi być możliwość stworzenia kont jedynie z uprawnieniami do podglądu – bez możliwości dokonywania zmian w systemie ani na urządzenia.
35. System musi posiadać funkcje zarządzania siecią wirtualną poprzez integrację z VMware (minimum wersja 6.0) i Microsoft Hyper-V(minimum w wersji 2012). Między innymi musi pozwalać na:
    a. Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem VMware ESX z wykorzystaniem protokołu SOAP.
    b. Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Virtual Machine Manager z wykorzystaniem Windows PowerShell.
    c. Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Hyper-V z wykorzystaniem protokołu WMI.
    d. Zarządzanie siecią wirtualną, w tym serwerami VMware vCenter Server oraz Microsoft Virtual Machine Manager, wirtualnymi maszynami oraz wirtualnymi przełącznikami.
    e. Migrację wirtualnych maszyn pomiędzy fizycznymi serwerami.
    f. Przedstawienie wszystkich zasobów, szczegółowych informacji o nich oraz ich wzajemnych relacji w środowisku wirtualnym. Wymaga się, aby był wgląd minimum w:
        - Listę wszystkich fizycznych serwerów VMware ESX oraz Microsoft Hyper-V dostępnych w sieci. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: producent, model, nazwa serwera, adres IP, informacje na temat Managera sieci wirtualnej, ilość pamięci RAM (wraz z poziomem wykorzystania), CPU (wraz z poziomem wykorzystania) oraz informację czy dany serwer wspiera funkcję migracji maszyn wirtualnych.
        - Listę wirtualnych przełączników przyporządkowanych do konkretnych serwerów VMware ESX oraz Microsoft Hyper-V. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa przełącznika, ilość wirtualnych portów.
        - Listę wirtualnych maszyn przyporządkowanych do konkretnych przełączników wirtualnych. Dodatkowo

	wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa wirtualnej maszyny, adres IP, stan maszyny (Running, Stopped, Suspended). g. Zmianę stanu (minimum: Start VM, Stop VM, Suspend VM, Reset VM) i parametrów wirtualnej maszyny takich jak: zasoby CPU, ilość pamięci RAM, ilość przestrzeni dyskowej. h. Dodawanie, klonowanie i usuwanie wirtualnych masz. i. Kreowanie szablonów służących do tworzenia nowych wirtualnych maszyn, gdzie można zdefiniować parametry początkowe takie jak: nazwę VMware ESX/Microsoft Hyper-V, zasoby CPU, ilość pamięci RAM, przestrzeń dyskową, system operacyjny wirtualnej maszyny. j. Dodawanie wirtualnych przełączników wraz z możliwością wyboru konkretnych kart sieciowych fizycznego serwera, do których będzie połączony wirtualny przełącznik. Dodatkowo musi istnieć możliwość „load balancingu" pomiędzy kartami sieciowymi co najmniej w oparciu o: IP hash, MAC hash, port fizyczny ruchu przychodzącego. Musi być także możliwość ustawienia kart sieciowych w trybie Active-Standby. 36. System musi posiadać funkcje zarządzania co najmniej dla 1000 predefiniowanych modeli urządzeń. Oprócz tego musi być możliwość wgrania dowolnej bazy MIB dla urządzeń sieciowych nie obsługiwanych domyślnie przez System 37. System musi posiadać funkcję automatycznej aktualizacji przez Internet. 38. System musi posiadać funkcje implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów. 39. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled) 40. System musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy 41. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych
Kompatybilność	Na liście kompatybilności systemu zarządzania znajdować się muszą co najmniej: • przełączniki HPE 5945 będące w posiadaniu Partnera Projektu • przełączniki HPE 5130 będące w posiadaniu Partnera Projektu • przełączniki Aruba 2540 będące w posiadaniu Partnera Projektu • przełączniki Aruba 2930 będące w posiadaniu Partnera Projektu • Aruba AP-365 będące w posiadaniu Partnera Projektu • HPE Proliant XL190r gen10 będące w posiadaniu Partnera Projektu • HPE Proliant DL380 gen9 będące w posiadaniu Partnera Projektu • Fortinet Fortigate będące w posiadaniu Partnera Projektu
Gwarancja	Minimum 60cio miesięczna gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Partner Projektu musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
Dodatkowe akcesoria	Mobilna stacja do monitoringu o parametrach nie gorszych niż: Komputer przenośny o przekątnej matrycy maks. 14", procesor 4ro rdzeniowy osiągający w teście PassMark CPU Mark wynik min. 10000 punktów (http://www.cpubenchmark.net), 8GB RAM z możliwością rozbudowy do 32GB,

	rozdzielczość Full HD, dysk m.2 o pojemności min. 256GB, min. 3 złącza USB 3.0 Typ A, 1x HDMI, 1x Thunderbolt 4, 1x RJ-45, WiFi 802.11ax, wbudowany czytnik linii papilarnych, bateria o pojemności min. 45Wh, waga maks. 1.6kg, wysokość maks. 20.5mm, szerokość maks. 331mm, głębokość maks. 236mm, oprogramowanie Systemowe Windows 10 Pro lub równoważne w pełni wspierające obsługę MS ActiveDirectory

1.5 Serwer poczty elektronicznej - 1 szt.

Wymagania ogólne

Dostarczony system pocztowy musi zapewniać wszystkie wymienione poniżej funkcje.

Dostarczone system powinien pracować w trybie wysokiej dostępności (HA Active-Pasive oraz HA Active-Active).

Dostarczone urządzenie powinno dawać możliwość połączenia w klaster HA z urządzeniem Fortinet Fortimail 400F będącym w posiadaniu Partnera Projektu. Partner Projektu posiada urządzenie Fortimail 400F (numer seryjny jest tajemnicą przedsiębiorstwa i zostanie przekazany Wykonawcy po podpisaniu Umowy) z gwarancją i wsparciem producenta do dnia 24 sierpnia 2022 roku. Zamawiający wymaga zrównania gwarancji, wsparcia producenta oraz licencji obecnie posiadanego urządzenia oraz nowego urządzenia dostarczanego w ramach klastra HA.

Zamawiający dopuszcza wymianę posiadanego urządzenia Fortinet Fortimail 400F pod warunkiem dostarczenia rozwiązania zapewniającego funkcjonalnie i wydajnościowo parametry nie gorsze niż opisane w tabeli poniżej i parametry nie gorsze od posiadanego przez Partnera Projektu urządzenia. W przypadku wymamiany wymagane jest dostarczenie min. dwóch urządzeń pracujących w trybie HA.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wymagania ogólne	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej)
Parametry fizyczne	1. System musi być wyposażony w interfejsy: • 4 porty Gigabit Ethernet RJ-45. 2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB z możliwością obsługi mechanizmu RAID 1 lub 5 lub 10. 3. System musi posiadać wbudowany port konsoli szeregowej.

	4. Zasilanie z sieci 230V/50Hz.
Funkcje serwera poczty	W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych. Dostarczony system musi zapewniać: 1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP. 2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2). 3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników. 4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3). 5. Polski interfejs użytkownika przy dostępie przez WebMail. 6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP. 7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
Ogólne funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 100 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 150 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail lub IMAP. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.

	14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). 18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
Kontrola antiwirusowa	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake.
Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Filtrowanie treści wiadomości i załączników. 10. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 11. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. 12. Ochrona typu outbrake.

	13. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 14. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora
Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
Funkcje pracy w trybie HA	System ochrony poczty musi zapewniać poniższe funkcje: 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.
Aktualizacja sygnatur	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.

	3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
Certyfikaty	Dostarczony system powinien posiadać co najmniej jedną z poniższych certyfikacji: 1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified
Serwis I licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 60 miesięcy
Gwarancja oraz wsparcie	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

1.6 Macierz do przechowywania kopii zapasowych - 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ obudowy	Macierz musi być przystosowany do montażu w szafie rack 19”, o wysokości maksymalnie 4U.
Przestrzeń dyskowa	Min. 20 zatok na dyski Macierz musi udostępniać minimum 300 TB przestrzeni użytkowej z zabezpieczeniem na poziomie RAID5 zbudowanej w oparciu o minimum 20 dysków.
Obsługa dysków	Serwer musi obsługiwać dyski SSD, SATA. Serwer musi umożliwiać mieszanie napędów dyskowych SSD i SATA w obrębie pojedynczej półki dyskowej. Serwer musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	• Serwer musi obsługiwać mechanizmy JBOD, RAID 0, 1, 5, 6, 10, • Global Hot Spare • Rozszerzenie pojemności RAID w trybie online • Zmiana typu RAID w trybie online • Szyfrowanie danych min. AES 256 (folderów i volumenów) • Backup na zewnętrzny storage (USB) • Obsługa snapsohotów • Synchronizacja plików pomiędzy urządzeniami mobilnymi
Pamięć i procesor	Min. 16 GB RAM (z możliwością rozbudowy do min. 128GB) Procesor min. 6 rdzeniowy osiągający w teście PassMark CPU Mark wynik min. 9300 punktów (**http://www.cpubenchmark.net**)

Interfejsy	Min. 4 porty 1G RJ45 min. 2 porty 10G SFP+ min. 2 gniada PCIe Gen3 (min. 1szt x8)
Sieć	Możliwość tworzenia wirtualnych przełączników Obsługa IPv4 oraz IPv6 Obsługa DHCP (server i client), STP, Link aggregation, DDNS Obsługa statycznego routingu Obsługa ramek Jumbo
Porty USB	Min. 2 porty USB 3.0
Zasilanie	Zainstalowane min. 2 redundantne zasilacze
Wspierane systemy plików	EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Udostępniania plików	Udostępniania plików dla: Windows, Mac, and Linux/UNIX Protokoły: CIFS/SMB 3, AFP, NFS v4, FTP, FTP over SSL / TLS, SFTP, HTTP, WebDAV, iSCSI, RSync, lokalna przeglądarka plików przez WWW Wsparcie dla Windows ACL
Obsługa użytkowników	Integracja z MS ActiveDirectory Obsługa ACL przy udostępnianiu plików Lokalne ACL Lokalna baza użytkowników Zaawansowane listy ACL dla folderów i podfolderów
Wsparcie wirtualizacji	Możliwość uruchamiania maszyn wirtualnych z systemem Windows, Linuks, Android, Unix Konsola zarządzania wirtualizacją oparta o technologię HTML5
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Zamawiający dopuszcza zaoferowanie jednostki głównej z dodatkowymi półkami dyskowymi. Menu w języku Polskim oraz w co najmniej w języku Angielskim.
Monitoring	Pojemność urządzenia, wydajność, kondycja zasobów Skanowanie Bad block S.M.A.R.T. Kontrola systemu plików

	Disk Scrubbing Defragmentacja dysku Powiadomienia poprzez SMTP, email, LCD, SNMP, syslog, lokalnie Automatyczne wyłączanie (dyski, wentylatory, UPS) Auto-restart po odzyskaniu zasilania
Oprogramowanie dodatkowe zapewniające szyfrowany backup w chmurze zgodnie z rekomendacją CSIOZ	**Analiza architektury i opis rozwiązania** 1. Przegląd procedur i uzupełnienie polityki zarządzania backupem w organizacji Partnera Projektu. 2. Weryfikację elementów mających zapewnić bezpieczeństwo przetwarzanych informacji (poufność, integralność i dostępność). 3. Przygotowanie rozwiązania dedykowanego do optymalizacji procesu backupu danych w trybie automatycznym na infrastrukturze Partnera Projektu. 4. Wykonanie testów pozwalających na ocenę prawidłowości i funkcjonalności zastosowanych procedur i rozwiązań. 5. Wykonywanie backupów w trybie cyklicznym zgodnie z ustaloną polityką. 6. Czasowe użyczenie licencji na okres 12 miesięcy oprogramowania służącego do szyfrowania i bezpiecznego składowania danych Partnera Projektu w przestrzeni 1 TB z możliwością zwiększenia. 7. Czasowe użyczenie licencji na okres 12 miesięcy oprogramowania służącego do bezpiecznego przesyłania i współdzielenia plików w ramach struktury organizacyjnej Partnera Projektu dla 1 komputera z możliwością zwiększenia. 8. Rozwiązanie technologiczne musi być zgodne z: • „Rekomendacjami Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej" i • Kodeksem postępowania dla sektora ochrony zdrowia wydanym zgodnie z art. 40 RODO dotyczącym podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających i jednocześnie: a. posiadać moduł bezpiecznego przesyłania, jak również współdzielenia wszystkich rodzajów i wielkości plików w ramach struktur organizacyjnych jednostki oraz możliwość współdzielenia i przesyłania plików z podmiotami zewnętrznymi za pomocą oprogramowana, b. być rozwiązaniem bezpiecznym opartym o technologię kryptograficznej ochrony danych, gwarantującej podwyższony poziom ochrony prywatnych kluczy szyfrujących, który realizowany będzie poprzez technologię zapewniającą, że nie będą one nigdy przetrzymywane w całości w jednym miejscu, c. zapewnić przesyłanie i współdzielenie plików na urządzeniu klienckim z wykorzystaniem mocy obliczeniowej zarówno jego mikroprocesora, jak i częściowo mocy obliczeniowych mikroprocesorów wykorzystywanych przez serwery, które będą wykorzystywane do bezpiecznego przesyłania i współdzielenia plików, o których mowa, d. gwarantować wysoki poziom ochrony symetrycznych kluczy kryptograficznych przechowywanych na serwerach z

	wykorzystaniem mechanizmu kapsułkowania klucza (Key Encapsulation Mechanism), e. zagwarantować, że wszelkie pliki, które klient umieszcza na serwerze przechowywane i wysyłane będą w formie zaszyfrowanej, f. zagwarantować, że serwer nie jest w stanie uzyskać dostępu do plików klienta w postaci jawnej (serwer nie posiada, ani nie może wyznaczyć żadnego z kluczy kryptograficznych klienta usługi), g. gwarantować, że klient nie jest w stanie wykonać żadnej operacji kryptograficznej na swoim kluczu prywatnym (podpisu, deszyfrowania) bez udziału serwera, h. posiadać współdzielony dysk z możliwością nadawania uprawnień poszczególnym użytkownikom, do którego będzie możliwe dodawanie i przechowywanie plików w formie zaszyfrowanej, i. zapewniać wysyłanie do określonych użytkowników zaszyfrowanych plików, w tym do pojedynczego odbiorcy jak również grupy odbiorców, j. zapewniać szyfrowanie wybranych plików na lokalnych i sieciowych dyskach stacji roboczej, k. zapewnia szyfrowanie z umieszczeniem na serwerze wybranych plików i folderów z poziomu stacji roboczych, l. zapewniać współpracę z systemem operacyjnym Microsoft Windows w wersji 10 PL (32-bit, 64-bit) i w wersji starszej jakim jest MS Windows 7 (32-bit, 64-bit), m. współpracować z urządzeniami mobilnymi tj. laptop, tablet z zainstalowanymi systemami operacyjnymi Microsoft Windows w wersji 10 PL (32-bit, 64-bit) i w wersji starszej jakim jest MS Windows 7 (32-bit, 64-bit). n. posiadać interfejs użytkownika w postaci dedykowanej aplikacji na stacjach roboczych, o. umożliwiać zarządzanie oprogramowaniem i użytkownikami w nim zdefiniowanymi, p. pozwalać lokalnie definiować uprawnienia z poziomu użytkownika do poszczególnych zasobów, q. posiadać kontrolę logowania do konta użytkownika (np. blokowanie logowania na konta prywatne) oraz ograniczać dostęp do konta użytkownika tylko dla wskazanego urządzenia (lub urządzeń), r. realizować połączenie za pomocą mechanizmów asymetrycznych oraz symetrycznych., s. zapewniać szyfrowanie na stacjach roboczych użytkownika, t. klucz prywatny nie jest przechowywany w jednym miejscu (na stacji roboczej lub serwerze) z wyjątkiem momentu generowania klucza na stacji roboczej, u. zapewniać szyfrowanie kanału transferu danych na poziomie równym lub wyższym niż technologia Point to Point Tuneling Protocol. v. interfejs graficzny musi posiadać cechy ułatwiające użytkownikowi zarządzanie informacją np.: cechy i wygląd podobny do klienta pocztowego tzn. posiadać skrzynkę nadawczą, odbiorczą, pozwalać na wpisanie tytułu wiadomości, adresatów, treści i dodawanie załączników.

	w. szyfrować end-to-end – współdzielone lub przesyłane pliki muszą być szyfrowane i przekazywane zawsze w postaci zaszyfrowanej. x. Posiadać funkcjonalność automatycznej synchronizacji szyfrowanych folderów serwera z folderem lokalnym stacji roboczej w kontekście każdego konta użytkownika. Synchronizowany folder musi być dostępny dla użytkownika dopiero po poprawnym zalogowaniu do systemu. y. Posiadać funkcjonalność wersjonowania plików tak by każdy uprawniony użytkownik mógł przywrócić poprzednią wersję pliku. System musi umożliwiać przywrócenie dowolnej archiwalnej wersji jako wersję aktualną. z. Posiadać funkcjonalność „kosza", który przechowuje wszystkie usunięte przez użytkownika pliki i umożliwia ich przywrócenie. aa. Umożliwiać automatyzację procesów logowania, szyfrowania, przesyłania danych przez zastosowanie API. **Zasady świadczenia wsparcia oraz opieki serwisowej** Wykonawca zobowiązany jest w trakcie trwania umowy licencyjnej: 1. Dostarczać Partnerowi Projektu nowsze wersje oprogramowania, uaktualnienia oraz „support packi" poprzez wskazanie miejsca do pobrania i przesłania informacji drogą mailową, wraz z instrukcją instalacji i listą zmian – release notes; 2. Świadczyć usługi opieki serwisowej oraz wsparcia oprogramowania także na nowszych wersjach oprogramowania – dostarczonych w ramach umowy; 3. Udzielić wsparcia w trakcie instalacji dokonywanych przez Partnera Projektu dostarczonego oprogramowania oraz poprawek; 4. Zapewnić rozwiązywanie problemów związanych z instalacją i funkcjonowaniem dostarczonego oprogramowania; 5. Zapewnić przyjmowanie zgłoszeń telefonicznych potwierdzanych zgłoszeniem elektronicznym (www lub e-mail) w trybie 24x7x365 od Partnera Projektu z zachowaniem minimalnych warunków przyjęcia zgłoszenia, przez Wykonawcę, tj.: • w godzinach pomiędzy 08:00 a 16.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte danego dnia roboczego; • w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – zgłoszenie traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego; • w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 danego dnia roboczego; • w dniu ustawowo lub dodatkowo wolnym od pracy - zgłoszenie traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego; 6. Nie później niż w ciągu 30 minut od momentu otrzymania zgłoszenia awarii potwierdzić przyjęcie zgłoszenia; 7. Zapewnić czas reakcji na zgłoszone problemy, rozumiany jako przesłanie szczegółowego planu działania naprawczego Wykonawcy w związku z dokonanym zgłoszeniem przy zgłoszeniu: a. błędu krytycznego do 12 godzin od momentu zgłoszenia, b. błędu niekrytycznego naprawa powinna nastąpić w najbliższym wydaniu oprogramowania.

	Status zgłoszenia określa Partner Projektu, wg poniższych kryteriów: a. błąd krytyczny – nie można zaszyfrować/odszyfrować danych; b. błąd niekrytyczny – pozostałe błędy; 8. Zapewnić dostęp do bazy wiedzy o dostarczonym oprogramowaniu; 9. Zapewnić e-mail'owe i telefoniczne konsultacje w zakresie dostarczonego oprogramowania we wszystkie dni robocze w godz. 9.00 – 17.00 **Dokumentacja** W ramach realizacji projektu, Wykonawca opracuje i dostarczy m.in. szczegółową dokumentację dotyczącą instalacji, konfiguracji i parametryzacji Systemu do szyfrowania danych oraz konfiguracji stacji roboczych wraz z opisem procedur i instrukcji eksploatacyjnych. 1. Wykonawca przygotuje: 1.1. Procedury i instrukcje instalacji i rejestracji licencji. 1.2. Procedury i instrukcje odzyskiwania kont użytkowników. 1.3. Procedury i instrukcje bieżącego monitoringu zasobów serwerowych. 1.4. Procedury i instrukcje aktualizacji i wdrażania łat. 1.5. Politykę szyfrowania danych na stacjach roboczych. 1.6. Metody odzyskiwania danych zaszyfrowanych lokalnie oraz na nośnikach zewnętrznych. 1.7. Opis ról i ich uprawnień do Systemu. 1.8. Procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów. 1.9. Procedury tworzenia płyty CD/DVD i pendrive z oprogramowaniem do odzyskiwania danych. W przypadku konieczności użycia do tworzenia płyty CD/DVD i pendrive oprogramowania firm trzecich, Wykonawca w ramach niniejszego projektu, bez dodatkowych kosztów dla Partnera Projektu, dostarczy i przekaże na jego rzecz to oprogramowanie wraz z licencjami umożliwiającymi jego użytkowanie przez okres subskrypcji dla ilości zgodnej z ilością licencji. 1.10. Instrukcje obsługi Systemu do szyfrowania danych dla: Użytkowników oraz Administratorów. 2. Dokumentacja będzie weryfikowana i w razie potrzeby zaktualizowana po każdej modyfikacji/ aktualizacji Systemu do szyfrowania danych. 3. Dokumentacja dotycząca czynności administracyjnych związanych z utrzymaniem Sytemu do szyfrowania danych musi być dostarczana niezwłocznie wraz z nową wersją Systemu. Pozostała dokumentacja może być dostarczona nie później niż w terminie 14 dni od daty przekazania nowej wersji Systemu.
Gwarancja	Wymaga się aby urządzenie było objęte min. 5 letnią gwarancją producenta realizowaną w systemie door-to-door przez serwis producenta lub dystrybutora

1.7 Dysk SSD do Serwerów Apollo 2x00 - 24 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Dysk SSD 2.5”	Dysk SSD o pojemności RAW min. 1.92TB przeznaczamy do serwera Apollo 2800 będącego w posiadaniu Partnera Projektu.
Gwarancja	Gwarancja: 60 miesięcy

PN serwerów Apollo 2x00, do których mają zostać dostarczone dyski SSD: 867159-B21. Numery seryjne serwerów Apollo 2x00 są tajemnicą przedsiębiorstwa i zostaną przekazany Wykonawcy po podpisaniu Umowy.

1.8 Serwer wirtualizacyjny - 4 kpl.

Wymagania ogólne dotyczące sprzętu serwerowego:

a) Gdziekolwiek w opisie przedmiotu zamówienia przywołane są normy, lub nazwy własne lub znaki towarowe lub patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę Partner Projektu dopuszcza rozwiązania równoważne.
b) Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2008 lub normą równoważną.
c) W momencie oferowana wszystkie elementy oferowanej architektury muszą być dostępne (dostarczane) przez producenta.
d) Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
e) Urządzenia muszą być dostarczone Partnerowi Projektu w oryginalnych opakowaniach fabrycznych.
f) Do każdego dostarczonego wraz z serwerem systemu operacyjnego muszą być załączone oryginalne dokumenty licencyjne uprawniające do używania systemu operacyjnego określonego dla każdego z serwerów
g) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.
h) Wszystkie serwery muszą posiadać Certyfikat CE produktu albo spełniać normy równoważne.
i) Oferowane serwery muszą być przygotowane do współpracy z systemami operacyjnymi takimi jak: Microsoft Windows Server 2019, LINUX Red Hat, Vmware, Microsoft Windows Server 2016, HyperV
j) Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach : 230 V ± 10% , 50 Hz.
k) Sprzęt powinien być objęty gwarancją producenta sprzętu przez okres zgodny z wymaganiami zamieszczonymi w poniższych rozdziałach. .
l) Wszystkie poniższe parametry należy traktować jako minimalne.
m) Wszelkie użyte nazwy własne producentów należy traktować informacyjnie i dopuszczona jest możliwość zastosowania technologii w inny sposób zapewniających poniższe funkcjonalności.

Zaprojektowano 4 komplety serwerów jako środowisko produkcyjne z wykorzystaniem wirtualizatora, które będzie uruchamiało maszyny wirtualne potrzebne do obsługi informatycznej Szpitala. Serwery te będą pracowały z wykorzystaniem funkcji klastra HA.

Każdy z serwerów powinien mieć następującą konfigurację:

- Obudowa o wysokości maksymalnie 2U z zestawem umożliwiającym montaż w szafie rack 19”
- Min. dwa procesory min. 8 rdzeniowe
- Pamięć RAM min. 256GB typu Registered

- Płyta główna dedykowana do pracy w serwerach
- Karta sieciowa z min. 2 portami 25G zakończone złączem SFP28
- Karta sieciowa z min. 2 portami 10G zakończone złączem SFP+
- Dedykowane dyski do instalacji wirtualizatora
- Karta graficzna zintegrowana na płycie głównej
- Dwa zasilacze redundantne, typu Hot-Plug
- Wentylatory redundantne, typu Hot-Plug

Serwery należy podłączyć do Zasilaczy Awaryjnych UPS zgodnie z opisem. Ponadto serwery należy podłączyć do dostarczonych przełączników sieciowych.
Na serwerach należy skonfigurować środowisko wirtualne.

Obudowa	Obudowa o wysokości maksymalnie 2U. Obudowa musi być przystosowana do montażu w standardowej szafie Rack 19” i zawierać komplet kabli połączeniowych niezbędnych do instalacji. Obudowa umożliwiająca instalację minimum 24 dysków Hot Plug 2.5” - w pełni wspierająca skonfigurowanie co najmniej 24 dysków dla jednostki przetwarzania. Obudowa umożliwiająca instalację minimum 12 dysków NVMe 2.5”. Zainstalowane min. 24 dyski SSD 2.5” o pojemności sumarycznej RAW min. 190TB. Nie dopuszcza się mieszania dysków różnej pojemności. Zasilanie redundantne, jednofazowe o min. mocy 800W. Obudowa musi umożliwiać instalację redundantnych wentylatorów. Obudowa musi umożliwiać instalację min. 4 procesorów Obudowa musi umożliwiać instalację min. 6TB pamięci RAM DDR4 Wymagane jest dostarczenie oryginalnej maskownicy producenta przykrywającej dyski (front obudowy) **Obudowa musi pozwalać na instalację serwera HPE ProLiant XL190R Gen10 będącego w posiadaniu Partnera Projektu.**
JEDNOSTKA PRZETWARZANIA	
Płyta główna, chipset	Płyta główna z możliwością zainstalowania co najmniej dwóch procesorów. Chipset dedykowany przez producenta procesora do pracy w serwerach min. dwuprocesorowych. Konfiguracja umożliwiająca instalację maksymalnej ilości procesorów i pamięci, dostępnej dla zaoferowanej modelu jednostki przetwarzania, bez konieczności uzupełniania o jakiekolwiek elementy.
Procesory	Wszystkie gniazda procesorów obsadzone przez procesory ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem. Każdy z procesorów osiągający w teście PassMark CPU Mark wynik min. 21000 punktów (http://www.cpubenchmark.net)
Pamięć RAM	Dla każdego procesora zainstalowane co najmniej 256GB pamięci RAM typu RDIMM o częstotliwości pracy 2666MT/s. w modułach co najmniej po 32GB. Płyta musi obsługiwać minimum 1.5TB pamięci RAM. Płyta główna umożliwiająca instalacje min. 8 kości pamięci dla każdego procesora. Możliwe zabezpieczenia pamięci: ECC, Memory Mirror lub równoważne.

Pamięć masowa	Zainstalowane min. dwa dyski M.2 SSD SATA o pojemności minimum 240GB każdy (skonfigurowane w RAID 1).
Kontroler dysków	Co najmniej 1 kontroler obsługujący RAID 0, 1, 5, 10. Możliwość dokupienia licencji na szyfrowanie dysków.
Połączenia sieciowe	Minimum 2 porty 25GbE SFP28 (min. dwa porty powinny zostać obsadzone wkładkami SFP+ 10Gb LR w pełni kompatybilnymi z dostarczanym serwerem). Minimum 2 porty 10GbE SFP+ (min. dwa porty powinny zostać obsadzone wkładkami SFP+ 10Gb LR w pełni kompatybilnymi z dostarczanym serwerem). Karta/y sieciowe powinny być sygnowane przez producenta serwera i opisane w oficjalnych dokumentach producenta (DataSheet)
Złącza PCI-E	Minimum 2 złącza PCI-E 3.0 x16.
Inne porty	Minimum 2 porty USB (na zewnątrz) w tym minimum 1 x USB 3.0, 1x Wideo (zintegrowana karta graficzna oferująca minimalną rozdzielczość 1280x1024 lub możliwość uzyskania portu wideo przy użyciu przejściówki).
Wspierane systemy operacyjne	Serwer musi znajdować się na liście zgodności systemów: SUSE Linux Enterprise Server (SLES) 11 SP4 i 12 SP2 Red Hat Enterprise Linux (RHEL) 6.9 i 7.3 Windows Server 2019 Windows Server 2016 VMware ESXi 6.5
Bezpieczeństwo	Możliwość wyposażenia serwera w zintegrowany z płytą główną moduł TPM.
System operacyjny	Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego. • Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 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: o pozwalają na zmianę rozmiaru w czasie pracy systemu, o umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, o umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, o 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: o Login i hasło, o Karty z certyfikatami (smartcard), o 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: O Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, O 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 8.1. o Zdalna dystrybucja oprogramowania na stacje robocze. o Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej o Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: o Dystrybucję certyfikatów poprzez http o Konsolidację CA dla wielu lasów domeny, o Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, o Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. o Szyfrowanie plików i folderów. o Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). o Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. o Serwis udostępniania stron WWW. o Wsparcie dla protokołu IP w wersji 6 (IPv6), o Wsparcie dla algorytmów Suite 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.
System wirtualizacyjny	**2.2.1.** Wirtualizacja mocy obliczeniowej: Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym oraz musi spełniać poniższe warunki: o Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 512 logicznych wątków oraz do 12TB pamięci fizycznej RAM o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-8 wirtualnych kart sieciowych o Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 2 porty szeregowe

	o Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2008/2008R2, Windows Server 2012/2012R2, Windows Server 2016, Windows 7, Windows 8.1, Windows 10, SLES 12, SLES 11, REHL 7, RHEL 6, RHEL 5, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux o Rozwiązanie musi umożliwiać przydzielenie pamięci RAM dla maszyn wirtualnych w sposób pozwalający na obsługę większej ilości pamięci niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji o Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych o Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, na maszynie wirtualnej o Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania o Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez bezpieczny szyfrowany kanał, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta głównego (root/Administrator) o Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania/eksportowania systemów operacyjnych wraz z ich konfiguracją i danymi o Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych wirtualnych instancji systemów operacyjnych bez przerywania ich pracy z możliwością zachowania stanu pamięci pracującej maszyny wirtualnej. o Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory lub Open LDAP o Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości pamięci operacyjnej i pojemności przydzielonej przestrzeni dyskowej o System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE o System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych o System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów o Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w

	razie awarii karty sieciowej o Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN), zapewniające również separację warstwy trzeciej o Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi o Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek o Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych wirtualnych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie o Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z serwerów fizycznych na serwery w tym samym lub oddalonym ośrodku przetwarzania o Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi o Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury o Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych o Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania o Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to poprawki bezpieczeństwa, bez potrzeby wyłączania wirtualnych maszyn o Rozwiązanie musi posiadać co najmniej 2 niezależne. mechanizmy wzajemnej komunikacji między serwerami, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci o Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie o Oprogramowanie do wirtualizacji musi obsługiwać SAN o Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB o Rozwiązanie musi posiadać możliwość integracji zewnętrznych rozwiązań wykonywania kopii zapasowych o Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do wirtualizacji pamięci masowej (SDS) oraz wirtualzacji sieci (SDN). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami)

	o System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader o Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów o Licencja na oprogramowanie spełniające powyższe wymagania musi pochodzić z oficjalnego polskiego kanału sprzedaży i być fabrycznie nowa, nigdy nie zarejestrowana czy wykorzystywana. Licencje dostępne w modelu licencjonowania na procesor/rdzeń fizyczny. o Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej o Rozwiązanie powinno posiadać proaktywny/heurystyczny mechanizm, który migruje wirtualne maszyny po wykryciu wzrostu obciążenia lub potencjalnego problemu z serwerem fizycznym. o System/SDS musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich o Rozwiązanie musi umożliwiać szyfrowanie wirtualnych maszyn **2.2.2.** Zarządzanie środowiskiem wirtualnym o Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej jak i wirtualnej. o Konsola graficzna musi być dostępna za pomocą przeglądarek. o Każda instancja konsoli może zarządzać dowolną ilością serwerów fizycznych na której zainstalowane jest oprogramowanie do wirtualizacji (brak ograniczeń licencyjnych). o Rozwiązanie musi zapewniać monitorowanie urządzeń w trybie „Real Time” **2.2.3.** Wirtualizacja funkcji sieciowych – SDN o Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne o Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej o Rozwiązanie musi posiadać funkcję wirtualnego routera, zapewniającego komunikację środowiska maszyn wirtualnych z siecią fizyczną. o Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN o Oferowane rozwiązanie musi posiadać pełną wymaganą funkcjonalność zarówno funkcji bezpieczeństwa oraz funkcji sieciowych w ramach rozwiązań jednego producenta o Rozwiązania musi posiadać funkcję rozproszonego, stanowego firewall’a, umożliwiającego definiowania reguł dla protokołów, portów i adresów.

	o Każdy serwer fizyczny na którym wykorzystywane jest oprogramowanie do wirtualizacji funkcji sieciowych musi obsługiwać dowolną ilość serwerów wirtualnych (brak ograniczeń licencyjnych). **2.2.4.** Wirtualizacja przestrzeni dyskowej – SDS o Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD o Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania" operacji odczytu / zapisu (Read/Write IO) po stronie serwerów fizycznych o Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności o Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania / dodatkowych maszyn wirtualnych. Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z zarządzaniem platformą wirtualizacyjną o Rozwiązanie musi zapewniać możliwość budowy wspólnej wysoko-wydajnej i wysoko-dostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 16 serwerów fizycznych o Rozwiązanie musi zapewniać obsługiwanie wolumenów/dysków wirtualnych maszyn do rozmiaru min. 32TB o Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache'ujący, dysk pojemnościowy o Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania. o Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi szafami rack/chassis o Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną listę wspieranych lub rekomendowanych konfiguracji. Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W

	przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawce/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery) o Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej o Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych o Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych, o Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych. o Rozwiązanie musi posiadać listę wspieranych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 5 niezależnych producentów sprzętu serwerowego dostępnego na rynku Unii Europejskiej. o System musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością o Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej. o Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla min.: technologii deduplikacji oraz technologii implementującej zabezpieczenie danych poprzez pojedynczą i podwójną parzystość za pomocą oprogramowania. o Rozwiązanie musi zapewniać automatyczne rebalansowanie i przywracanie bezpieczeństwa danych bez konieczności stosowania dedykowanych nadmiarowych dysków typu HotSprare, a wyłącznie przy wykorzystaniu wolnego miejsca na dostępnych nośnikach. o Każdy serwer fizyczny na którym wykorzystywane jest oprogramowanie do wirtualizacji przestrzeni dyskowej musi obsługiwać dowolną ilość serwerów wirtualnych (brak ograniczeń na serwery czy pojemność w jakimkolwiek aspekcie licencyjnym). **2.2.5.** Skalowanie całości platformy o Rozwiązanie musi udostępniać wspólny klaster mocy obliczeniowej i przestrzeni dyskowej, agregujący przetwarzanie danych, system rozproszonej pamięci masowej oraz serwerowy segment sieci. o Wirtualizacja mocy obliczeniowej musi pozwalać na połączenie pojedynczych node-ów serwerowych w klaster, umożliwiający bezprzerwowe przenoszenie maszyn pomiędzy serwerami fizycznymi, czy natychmiastowe ich przywracanie w przypadku jakiejkolwiek awarii na pozostałych node-ach klastra.

	o Wirtualizacja zasobów dyskowych musi całkowicie eliminować złożoną dedykowaną sieć pamięci masowej. Rozproszona pamięć masowa musi być niezależna od producentów sprzętu i stanowić wysokodostępne rozproszone, samolecząc się rozwiązanie. o Każdy serwer musi zostać wyposażony w zestaw licencji umożliwiający wykorzystanie wszystkich funkcjonalności opisanych jako wirtualizacji mocy obliczeniowej, wirtualizacja funkcji sieciowych, wirtualizacja przestrzeni dyskowej. Jeżeli wymagana jest licencja na system wirtualizacyjny, Wykonawca zobowiązany jest do dostarczenia odpowiedniej licencji pozwalająca na uruchomienie wszystkich opisanych wyżej funkcjonalności na dostarczanych serwerach. Licencja nie może być licencją typu Essentials tj. z ograniczeniem do maksymalnej ilości hostów.
ZARZĄDZANIE	
Zarządzanie	Niezależna od zainstalowanego na jednostce przetwarzania systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca centralne zarządzanie całą obudową z jednej konsoli: - 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 autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, SSH - obsługa RESTfull API - 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 - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
ZESTAW NIEZBĘDNY DO ZBUDOWANIA KLASTRA	
Zestaw	Zaoferowany zestaw musi zawierać wszystkie elementy niezbędne do zbudowania i uruchomienia klastra zgodnie z opisem funkcjonalnym. Licencje dostępowe do oprogramowania serwerowego: Jeżeli licencja na oprogramowanie operacyjne serwera wymaga od użytkownika końcowego posiadania licencji dostępowych (CAL), Wykonawca zobowiązany jest dostarczyć licencje na dostęp do serwerów dla minimum 300 użytkowników.
GWARANCJA	
Gwarancja	5-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w następnym dniu roboczym.

	W czasie trwania gwarancji, w przypadku uszkodzenia dysku Wykonawca powinien dostarczyć nowy dysk w ciągu 24 godzin od zgłoszenia uszkodzenia przez Partnera Projektu. Wykonawca powinien umożliwić Partnerowi Projektu zgłaszanie uszkodzeń dysku/ów w trybie 24/7 za pomocą dedykowanego portalu bądź numeru telefonu. W okresie gwarancji Partner Projektu ma prawo do otrzymywania poprawek oraz aktualizacji oprogramowania dostarczonego wraz z serwerem. Procedura serwisowa nie może wymagać od Partnera Projektu przeprowadzania testów sprzętu (np. sprawdzania sprzętu w podstawowej konfiguracji), całość procedur serwisowych musi zostać wykonana przez serwisanta.

Zamawiający posiada:

- serwery Apollo 2x00 serwerem XL190r o parametrach jak w OPZ, wyposażone w 24 dyski SSD 2TB każdy, Windows Server 2019 Datacenter
- serwery Apollo 2x00 z serwerem XL190r o parametrach jak w OPZ, wyposażone w 12 dysków SSD 2TB każdy, Windows Server 2016 Datacenter

PN serwerów Apollo: 867159-B21. Zamawiający dopuszcza wymianę istniejących urządzeń pod warunkiem dostarczenia urządzeń o parametrach nie gorszych od urządzeń opisanych w tabeli powyżej i parametrach nie gorszych od posiadanych przez Partnera Projektu urządzeń. W przypadku wymiany łączna ilość dostarczanych urządzeń to 8 sztuk wraz z niezbędnym wyposażeniem.

1.9 Zasilacz UPS dla punktów dystrybucyjnych - 15 szt.

Parametr	OPIS PARAMETRÓW
Obudowa	Możliwość montażu w szafie Rack 19” Wysokość max. 2U Głębokość maksymalnie 48cm
Moc	Min. moc pozorna: 1,5kVA Min. moc rzeczywista: 900W
Czas przełączenia	Maksymalny przeciętny czas przełączenia na baterię: 6ms
Złącza	Rodzaj i min. liczba wyjść: 4 IEC 320 C13 Rodzaj i min. liczba wejść: 1 IEC 320 C14 Porty komunikacji USB Port konsoli RJ-45
Czas podtrzymywania	Czas podtrzymania zasilania przy obciążeniu 450W przynajmniej 18 min., przy obciążeniu 900W przynajmniej 6min.
Architektura	Line interactive
Informacja o stanie pracy	Kontrola wizualna LCD Alarmy dźwiękowe: praca na baterii, konieczna wymiana baterii
Inne	Zimny start Układ AVR Sinus podczas pracy na baterii Napięcie wejściowe: 171-290V Głośność nie większa niż: 47dBA
Dołączone akcesoria	Podzespoły niezbędne do montażu zasilacza w szafie rack Oprogramowanie umożliwiające: monitorowanie stanu pracy UPS
Gwarancja	Gwarancja: 60 miesięcy

1.10 Centralny Zasilacz Awaryjny UPS 10 kVA - 2 kpl.

Parametr	OPIS PARAMETRÓW
Minimalne parametry	Moc znamionowa: 10kVA/10kW Napięcie wyjściowe 380V/400V/415V 3fazowe Nominalne napięcie wejściowe 380V/400V/415V 3fazowe Wyjściowy współczynnik mocy: 0,99 Sprawność w trybie podwójnej Konwersji: 95,5% Sprawność w trybie Ekonomicznym: 96% Przeciążalność: 1min dla 125%, 10min dla 110% THDI: <3,5%, Możliwość pracy równoległej Czas podtrzymania dla 10kW: min. 27 minuty Czas podtrzymania dla 5kW: min. 65 minuty Baterie wewnętrzne z możliwością instalacji/wymiany przez użytkownika bez udziału serwisu 5 styków komunikacyjnych w standardzie, komunikacja Modbus, UPS wyposażony w wyłączniki bypassu serwisowego Intuicyjny wyświetlacz LCD o przekątnej min.3,4” Głośność przy maksymalnym obciążeniu: maks. 60dBA Maksymalne wymiary WxSxG: 1400mm x 380mm x 930mm Masa maksymalna wraz z bateriami wewnętrznymi: 200kg
Dostawa i uruchomienie	Wykonawca ma obowiązek dostarczyć UPS w miejsce wskazane przez Partnera Projektu oraz dokonać instalacji oraz pierwszego uruchomienia w sposób przewidziany przez producenta.
Gwarancja	Gwarancja: 60 miesięcy

1.11 Oprogramowanie bazodanowe na potrzeby HIS – 2szt.

Oprogramowanie dedykowane do współpracy z systemem Comarch OptimedNXT będącym w posiadaniu Partnera Projektu

L.p.	Min. wymagania funkcjonalne
1.	Wykonawca dostarczy wymaganą ilość licencji systemu bazodanowego zgodną z konfiguracją serwerów bazodanowych
2.	System bazodanowy zostanie skonfigurowany w trybie HA
3.	Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows jak i Linux.
4.	Oferowany Motor bazy danych dla systemu HIS musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych.
5.	Oferowany Motor bazy danych dla systemu HIS posiada komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open source.
6.	Oferowany Motor bazy danych HIS ma możliwość realizacji kopii bezpieczeństwa w trakcie działania (na gorąco).

7.	Oferowany Motor bazy danych generuje kopie bezpieczeństwa automatycznie (o określonej porze) i na zadanie operatora oraz umożliwia odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
8.	Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
9.	Administrator posiada możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarzadzanie nimi może odbywać się z poziomu narzędzi do zarzadzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych).
10.	Hasła użytkowników są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej).
11.	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
12.	Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych
13.	Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego
14.	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.
15.	Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda prośba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.
16.	Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
17.	Możliwość migracji zestawu znaków bazy danych do Unicode
18.	Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
19.	Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych
20.	Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych
21.	Wsparcie protokołu XA
22.	Wsparcie standardu JDBC 3.0
23.	Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
24.	Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Po- winna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.
25.	Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
26.	Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być jeżykiem 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
27.	Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).
28.	Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej)

29.	Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. prośba wykonania instrukcji DDL, start serwera, stop serwera, prośba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).
30.	W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek
31.	Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych
32.	Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdza- nie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.
33.	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 może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.
34.	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
35.	Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup).
36.	Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.
37.	W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników
38.	Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX (ang. Portable Operating System Interface) dostępna z poziomu jeżyka SQL jak i procedur/funkcji składowanych w bazie danych.
39.	Możliwość budowy klastra na węźle obsługiwanym przez maksymalnie 2 procesory
Gwarancja	Minimum 60-cio miesięczna gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Partner Projektu musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

1.12 Oprogramowanie do zarządzania dostępem do sieci (NAC) - 1kpl.

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Funkcjonalność	System do kontroli dostępu musi charakteryzować się następującymi cechami: 1. Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor) 2. System musi odsługiwać minimum 1000 urządzeń klienckich (w tym gości) w trybie HA – klaster dwóch maszyn wirtualnych. Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia 3. Praca jako maszyna wirtualna 4. Musi posiadać wbudowany serwer Radius oraz TACACS + 5. Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym: a. Cisco Systems

	b. Fortinet c. Microsoft d. Alcatel-lucent Enterprise e. Aruba Networks f. Extreme Networks g. Producenta posiadanych przez Partnera Projektu urządzeń firm: Hewlett Packard Enterprise, Aruba Networks h. Producenta urządzeń opisanych w tym dokumencie 6. System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera. 7. System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. 8. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych. 9. Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych a. Microsoft Active Directory b. Radius c. Kerberos d. LDAP e. ODBC f. Współpraca z serwerami tokenów 10. Musi obsługiwać metody profilowania a. DHCP b. TCP c. MAC OUI d. SNMP e. Cisco device sensor 11. Wspierać protokoły a. Radius, Radius CoA, TACACS +, web authentication, SAML v2.0 b. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) c. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD) d. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP) e. EAP-TLS f. PAP, CHAP, MSCHAPv1 i v2, EAP-MD5 g. NAC, Microsoft NAP h. Windows machine authentication i. MAC Auth j. Audit (role oparte na porcie oraz skanowanie podatności) k. OCSP (Online Certificate Status Protocol) l. SNMP generic MIB, SNMP private MIB m. CEF (Common Event Format), LEEF (Log Event Extended Format) n. TLS 1.2 12. Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami 13. Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych: a. Co najmniej ESX 4.0, ESXi 4.1 do 6.0 b. Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise 14. - Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (1000). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte. 15. System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności a. Samodzielna rejestracja klientów gościnnych w oparciu o: • Adres e-mail • Numer telefonu (wiadomość SMS)

	• Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link) b. Logowanie w oparciu o portale społecznościowe c. Funkcja integracji z systemami trzecimi poprzez API d. Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową e. Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych. f. Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych. g. Funkcja personalizacji strony gościnnej 16. Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. a. Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działu IT b. System musi wspierać obsługę następujących systemów operacyjnych • MS Windows • Mac OS X • iOS • Android • Chromebook • Ubuntu c. Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci d. Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej e. Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu. f. Funkcja tworzenia unikalnych certyfikatów dla urządzeń. g. Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń h. Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID 17. Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. a. System kontroli końcówek klienckich musi mieć następujące funkcjonalności b. System musi wspierać następujące systemy operacyjne • Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis) • Apple Mac OS X 10.7 i nowsze • Red HAT Enterprise Linux 4 i nowsze • CentOS 4 (Community Enterprise Operating System) i nowsze • Fedora Core 5 i nowsze • SUSE linux 10.x i nowsze c. Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall d. Wyświetlanie informacji on-line o statusie monitorowanych końcówek e. System powinien obsługiwać agenta w formie • Stałej (Presistent Agent) • Tymczasowej (Dissolvabe Agent) • Agenta NAP
Gwarancja	Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez

	producenta sprzętu lub jego autoryzowany serwis. Partner Projektu musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
Testy	Partner Projektu może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Partnera Projektu w terminie nie dłuższy niż 2 tygodnie od chwili zażądania przez Partnera Projektu ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Partnera Projektu, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.
Inne	Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Partner Projektu zastrzega sobie prawo do weryfikacji spełnienia wymagań

1.13 Oprogramowanie do zarządzania zgłoszeniami - 1 kpl.

Nazwa komponentu	*Wymagane minimalne parametry techniczne*
Ogólne wymagania funkcjonalne	• System powinien posiadać obligatoryjnie interfejs Użytkownika w języku polskim. • Podczas rejestracji zgłoszenia przez Konsultanta SD, wypełnienie formularza danymi podstawowymi jak „Odbiorca Usługi” (dalej: Odbiorca), formularz zostanie automatycznie uzupełniony o dane dodatkowe: - umowa SLA, której Odbiorca podlega - lokalizacja Odbiorcy - miejsce Odbiorcy w strukturze organizacyjnej - dane kontaktowe: telefon komórkowy, telefon stacjonarny, adres email, według zdefiniowanych relacji. • Podczas wyszukiwania informacji z repozytoriów danych: ▪ System wyświetli formularz, który umożliwi użytkownikowi wprowadzenie danych, które posłużą do automatycznej konstrukcji zapytania wysyłanego do bazy Systemu. ▪ Na przykład: po wpisaniu do pola „Status” wartości „Powiązane” na formularzu wyszukiwania Zgłoszeń i wybraniu opcji „Wyszukaj”, System zwróci listę wszystkich Zgłoszeń o statusie „Powiązane”. ▪ System będzie umożliwiał dokonywanie zmian dostępnego zakresu informacji (pól) możliwych do wykorzystania na formularzach podczas wyszukiwania informacji. ▪ Wpisanie w pole formularza początkowych znaków spowoduje skonstruowanie zapytania, w znaczeniu „zaczynające się od”. ▪ Na przykład: po wpisaniu do pola „Nazwisko” wartości „A” na formularzu wyszukiwania Użytkowników i wybraniu opcji „Wyszukaj”, System zwróci

<table>
<tr>
<td></td>
<td>
listę wszystkich Użytkowników, których nazwiska zaczynają się od litery „A”.
• System będzie umożliwiał dodawanie nowych pól do tabel dla repozytoriów danych o typach:
<table>
<tr><th>Typ danych</th><th>Opis</th></tr>
<tr><td>Tekstowe</td><td>Pole umożliwiające wprowadzanie i przechowywanie ciągu dowolnych znaków alfanumerycznych</td></tr>
<tr><td>Numeryczne</td><td>Pole umożliwiające wprowadzanie i przechowywanie całkowitych wartości liczbowych</td></tr>
<tr><td>Daty</td><td>Pole umożliwiające wprowadzanie i przechowywanie wartości określających daty i czasy</td></tr>
<tr><td>Wielo-wierszowe</td><td>Pole umożliwiające wprowadzanie i przechowywanie wielu wierszy ciągu dowolnych znaków alfanumerycznych</td></tr>
<tr><td>Logiczne</td><td>Pole umożliwiające wprowadzanie i przechowywanie wartości prawda / fałsz</td></tr>
</table>
</td>
</tr>
<tr>
<td>Help Desk</td>
<td>
• System musi umożliwiać ręczną rejestrację zarówno prostych, szybkich do rozwiązania zgłoszeń jak i złożonych problemów opisujących rozległe awarie infrastruktury.
• System musi umożliwiać rejestrację zgłoszenia przez użytkownika końcowego z wykorzystaniem interfejsu www (który powinien automatycznie generować zapis Incydentu) poprzez tzw. Panel Klienta.
• System powinien generować zgłoszenia z sieci – automatyczne wysyłanie zgłoszeń do HelpDesk w przypadku wystąpienia awarii urządzeń w sieci komputerowej (możliwość).
• System musi udostępniać elastyczny mechanizm notyfikacji pozwalający definiować reguły powiadomień przypisanych operatorów w zależności od parametrów zgłoszenia.
• System musi uwzględniać pola obligatoryjne zgłoszenia: data i godzina Zgłoszenia, unikalny identyfikator Zgłoszenia (generowany automatycznie),
• System powinien umożliwiać definiowanie pól wypełnianych automatycznie: priorytet Zgłoszenia, data rejestracji Zgłoszenia, data przekazania Zgłoszenia do odpowiedniej Grupy Wsparcia, data realizacji, data zamknięcia, kontrolę zadeklarowanych parametrów realizacji.
• System musi mieć możliwość zdefiniowania wewnętrznych alarmów informujących o sytuacjach takich jak:
- zbliżający się termin rozwiązania;
- brak aktywności w kontekście wskazanych zgłoszeń.
• System musi umożliwiać operatorom tworzenie parametryzowanych kolejek zgłoszeń oraz dawać dostęp do kolejek zdefiniowanych przez administratorów.
• System powinien posiadać wewnętrzny mechanizm wysyłania wiadomości pomiędzy operatorami.
• System musi umożliwiać zgłaszającemu śledzenie postępu prac nad jego zgłoszeniami poprzez interfejs WWW.
</td>
</tr>
</table>

	• System musi posiadać Bazę Wiedzy z możliwością indeksowania przy użyciu słów klucz, dwupoziomowa baza wiedzy z oddzielnym dostępem dla serwisantów i klientów, grupowanie rozwiązań wg tematów i podtematów. • Narzędzie powinno posiadać widok „moje zadania" do tworzenia zadań dla serwisantów, ułatwiających zespołowi realizację. • Komunikacja z użytkownikiem powinna odbywać się poprzez automatyczne przesyłanie odpowiedzi do użytkownika o przyjęciu zgłoszenia, jego zamknięciu lub innych zmianach procesu realizacji zgłoszenia. • System powinien zapewniać automatyczne przekazywanie spraw, tj. automatyczne przekazywanie zgłoszeń serwisantów, na podstawie ich typu. • System powinien zapewniać możliwość zmiany przypisanego do zgłoszenia Elementu Konfiguracji lub dodanie nowego Elementu Konfiguracji w czasie obsługi zgłoszenia. • System powinien zapewniać możliwość sprawnego zarządzania kalendarzem z uwzględnieniem dni świadczenia usługi dla każdej usługi zgodnie z deklarowanym czasami ich wsparcia, planowanych przerw w działaniu infrastruktury, harmonogram wszystkich Zmian, ukazaniu zależności i wzajemnego wpływu planowanych i realizowanych czynności, uławiającym koordynację wszelkich aktywności w ramach codziennej pracy pracowników HelpDesk.
Zarządzanie konfiguracją	• System musi umożliwiać przechowywanie informacji o nieograniczonej liczbie Elementów Konfiguracji w centralnym repozytorium. • Każdy z typów Elementów Konfiguracji musi mieć własną listę atrybutów opisujących dany element. Pola w rekordzie powinny być specyficzne dla danego typu Elementu Konfiguracji. • System musi umożliwiać śledzenie cyklu życia Elementów Konfiguracji od momentu zamówienia do wycofania z użycia. Dodatkowo musi istnieć dostęp do pełnej historii cyklu życia danego Elementu Konfiguracji (kiedy i kto zmieniał status Elementu Konfiguracji). • Baza CMDB musi posiadać typowe klasy odpowiadające typowym elementom konfiguracji występującym w infrastrukturze informatycznej. Do typowych elementów konfiguracji zaliczamy: serwer, notebook, komputer PC, monitor, switch, router, drukarka. • System powinien umożliwiać zasilanie repozytorium Elementów Konfiguracji ze źródeł zewnętrznych. • System powinien dawać możliwość powiązania Elementów Konfiguracji z Incydentami. • Narzędzie powinno prezentować listę wszystkich zmian dotyczących Elementu Konfiguracji. • Dane o Elementach Konfiguracji muszą być dostępne dla Zgłoszeń, Incydentów, Problemów i Wniosków o Zmiany w trybie on-line. • System powinien umożliwiać propagowanie awarii Elementów Konfiguracji i ewentualnych przestojów związanych z tą awarią na powiązane z tym Elementem Konfiguracji inne Elementy. • System powinien umożliwić tworzenia relacji jeden-jeden, jeden-wielu, wiele-wielu na kilku poziomach pomiędzy Elementami Konfiguracji. Poprzez relację rozumiemy: ▪ Element Konfiguracji jest komponentem innego Elementu Konfiguracji; ▪ Element Konfiguracji wpływa na inny Element Konfiguracji; ▪ Element Konfiguracji należy do innego Elementu Konfiguracji;

	▪ Element Konfiguracji zależy od innego Elementu Konfiguracji
Zarządzanie poziomem usług	• System musi umożliwiać stworzenie centralnego repozytorium umów SLA wraz z opisem metryk w nich zawartych. • System powinien umożliwić dodawanie, modyfikację i usuwanie umów: - umowa z odbiorcą usług IT (Umowa SLA); • System powinien wspierać priorytetyzację rozwiązywania problemów w celu zapewnienia realizacji poziomu parametrów zapisanych w umowach SLA. • Powinna istnieć możliwość uporządkowania kolejek czynności do realizacji na podstawie priorytetu SLA. • System powinien umożliwiać powiadamianie o naruszeniu zdefiniowanego poziomu usługi w momencie wystąpienia naruszenia. • Proponowane rozwiązanie powinno umożliwiać utrzymywanie centralnego katalogu umów SLA wraz z informacjami opisującymi parametry poszczególnych umów. • System musi monitorować poziom spełnienia warunków określonych w umowach SLA. • System powinien umożliwić tworzenie reguł umów SLA dla użytkowników, departamentów, priorytetów lub kategorii i kontrolę ich przestrzegania. • System musi umożliwiać tworzenie dowolnej liczby kalendarzy czasu pracy np.: - pn-pt od 8:00 do 17:00; - pn-so 8:00 – 20:00; - 24 x 7; - inne dowolne godziny pracy w tygodniu. • System musi umożliwiać tworzenie wyjątków w kalendarzach pracy w postaci definiowania świąt i dni wolnych od pracy samodzielnie przez Administratora Systemu. • System musi posiadać funkcjonalność prezentującą wybrane lub wszystkie parametry definiujące Usługę IT użytkownikom końcowym.
Raportowanie	• System musi udostępniać możliwość samodzielnego budowania raportów w oparciu o bieżące potrzeby Partnera Projektu. • Narzędzie musi udostępniać graficzne narzędzie do projektowania raportów. • System musi posiadać możliwości definiowania prostych raportów ad-hoc przez użytkowników końcowych z możliwością ich zapisania do kolejnego użycia. Raportowanie ad-hoc powinno umożliwiać wybór danych tworzących kolumny raportu, kolumny do grupowania i sortowania. • System musi posiadać wbudowaną funkcjonalność graficznego prezentowania wybranych metryk. Uprawnieni użytkownicy powinni mieć możliwość definiowania własnych metryk.

	● Narzędzie musi mieć możliwość definiowania graficznej reprezentacji zestawu danych. ● Narzędzie powinno umożliwiać definiowanie uprawnień do raportów.
Rodzaje raportów	● Funkcja HelpDesk: ▪ Liczba i historia zgłoszeń (całkowita, o danym statusie, podjęte przez poszczególnych pracowników, w podziale na medium, za pomocą którego dokonano zgłoszenie); ▪ Liczba i historia zgłoszeń rozwiązanych w zdefiniowanych w Umowach SLA, OLA parametrach (z prezentacją poszczególnych progów kontrolnych, w zadanym okresie, rozwiązane, zamknięte, w podziale na osoby rozwiązujące zgłoszenie z prezentacją czasu rozwiązania, w podziale na osoby rejestrujące zgłoszenie z prezentacją czasu reakcji); ▪ Liczba i historia zgłoszeń o przekroczonych parametrach zdefiniowanych w Umowach SLA (z prezentacją poszczególnych progów kontrolnych, w zadanym okresie, rozwiązane, zamknięte, w podziale na osoby rozwiązujące zgłoszenie z prezentacją czasu rozwiązania, w podziale na osoby rejestrujące zgłoszenie z prezentacją czasu reakcji); ▪ Ilość zgłoszeń rozwiązanych przez pracowników HelpDesk z podziałem na kategorię zgłoszenia, osób rozwiązujących; ▪ Średni Czas Rozwiązania zgłoszeń w danym okresie w podziale na osoby rozwiązujące; ▪ Średni Czas Rozwiązania zgłoszeń w danym okresie liczony dla całego HelpDesku; ▪ Liczba reklamacji zgłoszonych przez Użytkowników. ● Zarządzanie Incydentami: ▪ Liczba Incydentów zgłoszonych w danym okresie czasu; ▪ Liczba Incydentów zamkniętych w danym okresie czasu; ▪ Liczba Incydentów rozwiązanych w zadeklarowanych czasach realizacji w podziale na poszczególnych pracowników IT; ▪ Liczba Incydentów przeterminowanych w podziale na poszczególnych pracowników IT; ▪ Liczba Incydentów rozwiązanych przez poszczególnych pracowników IT; ▪ Liczba reklamacji zgłoszonych przez Użytkowników dotyczących rozwiązania Incydentów; ▪ Liczba Incydentów zgłoszonych w danym okresie czasu w podziale na poszczególne Usługi IT; ▪ Liczba Incydentów zgłoszonych w danym okresie czasu w podziale na poszczególne Elementy Konfiguracji. ● Zarządzanie Konfiguracją: ▪ Liczba wolnych licencji na oprogramowanie;

	▪ Lista Elementów Konfiguracji, które uległy zmianie w danym okresie czasu. ● Zarządzanie Poziomem Usług: ▪ Liczba zdefiniowanych Usług IT; ▪ Liczba dotrzymanych i niedotrzymanych parametrów świadczenia Usług IT
Wymagania ergonomiczne	System powinien: ● umożliwiać poprawną obsługę rozdzielczości: 1024x768, 1280x800, 1280x1024, 1400x1050, 1600x1200, 1440x900, 1680x1050, 1920x1200; ● zapewniać czytelność aplikacji: wszelkie przyciski, listy wyboru, opcje będą łatwo dostępne; ● umożliwiać dynamiczne definiowanie widoków list wyszukiwanych rekordów i dynamiczne określanie "kolumn" wyświetlanych rekordów bez konieczności programowania, tworzenia i modyfikowania pól przez wyszkolonych administratorów Systemu po stronie Partnera Projektu; ● umożliwiać sortowanie listy rekordów, według wybranej kolumny po kliknięciu w nagłówek kolumny; ● umożliwiać użytkownikom personalizowanie interfejsu, tzn. umożliwi zmianę miejsca wyświetlania komponentów interfejsu, np.: ekranu roboczego, obszaru nawigacyjnego, okna komunikatów, wykresów, itp. bez konieczności programowania; ● zapewniać dopasowanie do potrzeb Partnera Projektu tzn. system musi mieć możliwość dodawania i modyfikowania istniejących formularzy, możliwości dodawania i modyfikowania istniejących procesów; ● umożliwiać użytkownikom korzystanie z wielu okien wybranych funkcjonalności równocześnie; ● umożliwiać korzystanie ze schowka systemowego Windows metodą „kopiuj – wklej” (ang. copy – paste); ● umożliwiać korzystanie z mechanizmu „przeciągnij i upuść” (ang. drag & drop) przy modyfikacji formularzy; ● umożliwiać obsługę interfejsu zarówno za pomocą myszy jak i klawiatury
Bezpieczeństwo	● umożliwiać użytkownikom końcowym dostęp za pośrednictwem przeglądarki internetowej w tym bez potrzeby instalowania dodatkowego oprogramowania na stacji klienckiej; ● umożliwiać korzystanie z pełnej funkcjonalności systemu za pośrednictwem przeglądarki internetowej; ● wspierać przeglądarki internetowe: Firefox, Chrome, Opera; ● zapewniać dwukierunkową integrację z usługami e-mail pracujących w oparciu o następujące protokoły: -SMTP -POP3 -MAPI

Integracja	System powinien umożliwić: • zintegrowanie z systemami Microsoft Active Directory • zintegrowanie z systemami Poczty elektronicznej (wysyłania, przyjmowania, pobierania adresów mailowych z książki adresowej systemu pocztowego)
Gwarancja i wsparcie	• Minimum 60-cio miesięczna gwarancja (serwis) producenta. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. • Wsparcie Wykonawcy przez okres min. 60 miesięcy polegające na świadczeniu pomocy zdalnej w trybie24/7 w ilości min. 1h tygodniowo. • Gwarancja powinno pozwolić na pobieranie nowych wersji oprogramowania przez okres min. 60 miesięcy
Wdrożenie i konfiguracja	Wykonawca powinien: • zainstalować system w środowisku wirtualnym Partnera Projektu • skonfigurować integrację z MS ActiveDirectory Partnera Projektu • skonfigurować integrację z serwerem pocztowym Partnera Projektu • skonfigurować użytkowników oraz administratorów zgodnie z wytycznymi Partnera Projektu • skonfigurować powiadomienia • skonfigurować sposób eskalacji zgłoszeń • skonfigurować kategorie zgłoszeń

1.14 Kable światłowodowe – 2 kpl.

Wykonawca dostarczy kable światłowodowe w celu rozbudowy sieci strukturalnej, o której mowa w Rozdziale 3,

Kable światłowodowe do połączenia pomiędzy punktami dystrybucyjnymi a serwerownią główną

Parametr	**OPIS PARAMETRÓW**
Zastosowanie	połączenia wewnątrz budynkowe, między piętrowe połączenia punktów dystrybucyjnych i konsolidacyjnych serwerownie
Rodzaj włókna	jednomodowy
Liczba włókien	16
Długość	Zgodnie z Załącznikiem nr 4 do Umowy
Rodzaj tuby	Tuba luźna

Kable światłowodowe do połączenia pomiędzy serwerownią główną a zapasową

Parametr	OPIS PARAMETRÓW
Zastosowanie	połączenia wewnątrz budynkowe, między piętrowe połączenia punktów dystrybucyjnych i konsolidacyjnych serwerownie
Rodzaj włókna	jednomodowy
Liczba włókien	32
Długość	Zgodnie z Załącznikiem nr 4 do Umowy
Rodzaj tuby	Tuba luźna

2. Instalacja, konfiguracja i wdrożenie

2.1. Instalacja serwerów

W szafach RACK należy zainstalować dostarczane serwery Wszystkie urządzenia należy w odpowiedni sposób połączyć i okablować. Partner Projektu dysponuje dwiema szafami 42U o wymiarach 800x1200.

Okablowanie powinno zostać umieszczone w odpowiednich uchwytach do okablowania oraz w szczotkach kablowych. Ilość akcesoriów musi być dostosowana do potrzeb.

Okablowanie musi zostać opisane/oznaczone po każdej stronie. Każda końcówka kabla powinna zostać wyposażona w opis, który powinien zawierać nazwę urządzenia oraz port, do którego przewód jest podłączony po przeciwnej stronie. Wymaganie to dotyczy zarówno kabli służących do transmisji danych jak i do kabli zasilających.

Każdy z serwerów powinien zostać podłączony do co najmniej dwóch przełączników rdzeniowych za pomocą min. jednego linku światłowodowego 10G do każdego przełącznika. Ponadto serwery muszą zostać podłączone do przełączników rdzeniowych za pomocą min. 2 linków 100G (po jednym do każdego przełącznika rdzeniowego). Dla połączeń 25G musi zostać wydzielony osobny VLAN (bez dostępu dla ruchu użytkowników). Dedykowany VLAN musi zostać skonfigurowany do replikacji danych między serwerami.

Na serwerach należy skonfigurować adres IP do zarządzania za pomocą wbudowanych mechanizmów konsolowych (niezależnych od systemu operacyjnego)

2.2. Instalacja UPSów centralnych i zasilanie szaf serwerowych

Dostarczane UPSy 10KVa należy zainstalować w dwóch serwerowniach Partnera Projektu. Instalacja powinna zostać przeprowadzona przez certyfikowanego inżyniera producenta UPS w sposób rekomendowany przez producenta. Partner Projektu przygotuje rozdzielnię, z której należy zasilić UPSy. Do zadań Wykonawcy należeć będzie doprowadzenie okablowania z dedykowanej rozdzielni do Szaf Serwerowych jak i do UPS. Informacja dotycząca tras kablowych znajduje w Załączniku nr 4 do Umowy. Każda szafa powinna zostać wyposażona w zasilanie z min. dwóch linii (faz) z czego jedna linia powinna pochodzić bezpośrednio z rozdzielni, druga linia powinna posiadać zasilanie gwarantowane z UPS. Obie linie powinny zostać zakończone listwą zasilającą bądź PDU. Każda listwa bądź PDU powinna zostać oznaczona w sposób pozwalający na jednoznaczne określenie miejsca zasilania.

2.3. Konfiguracja przestrzeni dyskowej, klastra oraz wirtualizacji

Rozwiązanie musi udostępniać wspólny klaster przetwarzania danych i pamięci masowej. Koncepcja zakłada migrację z rozwiązań niezagregowanych do pojedynczej skonsolidowanej opartej na oprogramowaniu pojedynczego producenta platformy, agregującej przetwarzanie danych - wirtualizacja serwerów, system rozproszonej pamięci masowej oraz serwerowy segment sieci. Wirtualizacja przetwarzania danych, konsoliduje obciążenia by lepiej wykorzystać moc obliczeniową i zapobiega marnowaniu zasobów (CPU, RAM), których nie mógłby wykorzystać pojedynczy serwer. Wirtualizacja pozwala połączyć pojedyncze node-y serwerowe w klaster, umożliwiający bezprzerwowe przenoszenie maszyn pomiędzy serwerami fizycznymi czy natychmiastowe ich przywracanie w przypadku jakiejkolwiek awarii na pozostałych node-ach klastra.

Rozproszona pamięć masowa całkowicie eliminuje złożoną dedykowaną sieć pamięci masowej oraz nie wymaga jakiegokolwiek własnościowego sprzętu o ograniczonej dostępności. Rozproszona pamięć masowa musi być niezależna od producentów sprzętu i nie wymagań jakiejkolwiek współdzielonej infrastruktury, musi mieć możliwość obsługi bezpośrednio widocznych dla niej indywidualnych urządzeń pamięci masowej. Musi być to wysokodostępne rozproszone, samolecząc się rozwiązanie. Zapewnia poziom bezpieczeństwa danych, gwarantujący pełne trzy kopie każdego fragmentu danych, na niezależnych urządzeniach fizycznych.

Każda kopia danych musi być replikowana synchronicznie, tak by w każdej chwili możliwe było natychmiastowe wykorzystanie którejkolwiek z kopii z pewnością że jest ona identyczna z pozostałymi. Do rozmieszczania danych na poszczególnych dyskach nie może być wykorzystywany bezpośrednio żaden mechanizm typu RAID, dane w każdej zapisanej kopii powinny być dostępne natychmiast nawet w przypadku awarii, bez konieczności przeliczania sum kontrolnych itp. Rozwiązanie musi zapewniać automatyczne rebalansowanie i przywracanie bezpieczeństwa danych bez konieczności stosowania dedykowanych nadmiarowych dysków typu HotSpare, a wyłącznie przy wykorzystaniu wolnego miejsca na dostępnych nośnikach. Mechanizmy rozproszonej pamięci muszą dbać o to by najczęściej wykorzystywane dane były na najszybszych dostępnych nośnikach (NVMe PCIe, NVDIMM, SSD) oferując wydajność dedykowanych urządzeń przy jednoczesnej elastyczności pamięci współdzielonej.

System musi pozwalać na „rozciągnięcie" klastra na dwie odrębne szafy serwerowe, nawet w przypadku połączenia ich wyłącznie pojedynczym połączeniem sieciowym Ethernet, przy czym dla nominalnego trybu dystrybucji danych taki rozciągnięty klaster gwarantować musi ciągłość pracy nawet w przypadku awarii dowolnej połowy elementów klastra. Rozwiązanie musi być oparte o co najmniej 2 niezależne autonomiczne node-y. Rozproszona pamięć masowa musi zapewniać możliwość uruchomienia wolumenów o mieszanym zabezpieczeniu danych, pozwalających na zdefiniowanie w ramach tego samego wolumenu pojemności obsługiwanej w ramach pełnej kopii danych oraz pojemności dla której wykorzystywane jest parzystość, przy czym migracja danych pomiędzy tymi dwiema pulami musi odbywać się bez fizycznego przenoszenia danych wyłącznie przy wykorzystaniu operacji na metadanych i dodania sum kontrolnych.

Rozwiązanie musi wspierać maszyny wirtualne, ich wysoką dostępność oraz kopie migawkowe.

Wszystkie opisane funkcjonalności muszą zostać w całości objęte dostarczanym licencjami i nie mogą mieć ograniczenia na pojemność w jakimkolwiek aspekcie licencyjnym. Rozwiązanie musi umożliwiać rozbudowę dostarczonej konfiguracji nominalnej o dodatkowe pojedyncze podzespoły, jak dodatkowe dyski.

System plików macierzy rozproszonej musi wspierać oferowane mechanizmy wirtualizacji i zapewniać akceleracją operacji na wirtualnych dyskach maszyn w zakresie tworzenia i scalania oraz scalania kopii migawkowych. Musi mieć on wbudowane mechanizmy realtime tiering-u, a także wspólny dla całego klastra mechanizm Storage QoS co najmniej w zakresie OPs/MBps Limits (maximums) oraz IOPs Guarantees (minimums), z możliwością przypisania polisy do pojedynczego wirtualnego dysku.

- Platforma musi zostać zainstalowana bezpośrednio na sprzęcie fizycznymi udostępniać mechanizmy wirtualizacji i udostępniać klaster wysokodostępny.
- Muszą zostać wdrożone mechanizmy klonowania/eksportowania/kopii migawkowych systemów operacyjnych wraz z ich konfiguracją i danymi na platformie wirtualizacji.
- Instalacja musi obejmować mechanizm przydzielania i konfiguracji uprawnień z integracją z usługami katalogowymi Microsoft Active Directory.
- Wdrożenie musi obejmować uruchomienie wirtualnego przełącznika sieci wirtualnej i łączącego maszyny wirtualne i zapewniającego przyłączania do niego co najmniej dwóch fizycznych kart sieciowych wraz z obsługą wirtualnych sieci lokalne (VLAN).
- Połączenie wirtualnego przełącznika musi być zrealizowane poprzez agregację połączeń 10GbE.

- Muszą zostać uruchomione mechanizmy przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
- Muszą zostać uruchomione mechanizmy redundancji w przypadku awarii np. serwera fizycznego, przełączające na inne serwery infrastruktury.
- Muszą zostać uruchomione mechanizmy bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to poprawki bezpieczeństwa, bez potrzeby wyłączania wirtualnych maszyn.
- Wdrożony musi zostać mechanizm automatycznego równoważenia obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma.
- Uruchomiony musi zostać mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich.
- Musi zostać zaimplementowana centralna konsola graficzna do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
- Wdrożenie musi obejmować budowę wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych.
- Uruchomiony musi zostać mechanizm optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania".
- Rozwiązanie storage musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej.
- Rozwiązanie musi udostępniać wspólny klaster mocy obliczeniowej i przestrzeni dyskowej, agregujący przetwarzanie danych, system rozproszonej pamięci masowej oraz serwerowy segment sieci.

Klaster łącznie musi oferować co najmniej:

- 64 fizycznych rdzenie
- 1024 GB pamięci RAM, zbudowanej w oparciu o moduły pamięci wykorzystujące symetrycznie wszystkie kanały pamięci procesora.
- 380 TB przestrzeni użytkowej na dane na dyskach SSD, zbudowanej w oparciu o co najmniej 24 dyski SSD 2.5" w każdym serwerze.

Tak skonfigurowany klaster należy połączyć z istniejącym już klastrem HyperV (Windows Server 2016 Datacenter oraz Windows Server 2019 Datacenter). Z konsoli na obu klastrach widoczne muszą być wszystkie maszyny wirtualne. Ponadto między klastrami należy uruchomić replikację, która w przypadku awarii klastra pozwoli uruchomić maszyny na działającym klastrze. Przed wykonaniem jakichkolwiek operacji Wykonawca zobowiązany jest do weryfikacji konfiguracji oraz stanu istniejącego klastra (4 hosty na serwerach Apollo 2800, 2 z Windows 2019 Datacenter, 2 z Windows 2016 Datacenter). Do obowiązków Wykonawcy należy również zaktualizowanie oprogramowania systemowego na istniejącym klastrze w taki sposób, aby na wszystkich serwerach oprogramowanie było w równej wersji. Jeżeli podniesienie wersji systemu operacyjnego wiązało się będzie z potrzebą posiadania przez Partnera Projektu licencji na ten system, Wykonawca zobowiązany jest do dostarczenia licencji na 32 rdzenie (4 procesory po 8 rdzeni).

2.4. Konfiguracja urządzeń sieciowych

Dostarczone **urządzenie Firewall** należy zainstalować w serwerowni we wskazanym przez Partnera Projektu miejscu.

Dostarczone urządzenie należy połączyć w klaster HA z urządzeniem Fortigate 100F będącym w posiadaniu Partnera Projektu.

Na urządzeniach należy:

- wykonać konfigurację tuneli VPN IPSec
- wykonać konfigurację interfejsów fizycznych, VLANów, interfejsów IP
- wykonać konfigurację SSL VPN (wraz z ustawieniami webportali)
- wykonać konfiguracje kont użytkowników SSL VPN
- wykonać konfigurację administratorów urządzenia
- wykonać konfigurację polityk bezpieczeństwa (w tym profile AV, AC, IPS, DLP, Webfiltering)

- wykonać konfigurację routingu
- wykonać konfigurację DHCP
- wykonać konfigurację trybu HA

Ponadto należy przeprowadzić analizę środowiska sieciowego klienta oraz struktury placówki w celu odpowiedniego zaprojektowania struktury logicznej sieci (VLANów).

Nowe urządzenia muszą mieć połączenie z istniejącą infrastrukturą placówki, należy w odpowiedni sposób skonfigurować routing i polityki bezpieczeństwa.

Przełączenie pracy sieci na nowe urządzenia nastąpi po uzgodnieniu terminu z Partner Projektu. Partner Projektu dostarczy informacje niezbędne do konfiguracji (hasła, adres IP itp.)

Dostarczone **urządzenia Firewall** należy podłączyć do dostarczonych przełączników szkieletowych. Każdy firewall musi zostać podłączony co najmniej jednym linkiem 10G do każdego z przełączników szkieletowych.

Przełączniki szkieletowe należy skonfigurować w trybie HA – stack, urządzenia muszą być widoczne w sieci jako jedno urządzenie logiczne. Połączenie między przełącznikami szkieletowymi musi zostać wykonane za pomocą min. 2 linków 100G.

Przełączniki dostępowe muszą zostać zainstalowane we wskazanych przez Partnera Projektu szafach RACK. Każdy przełącznik dostępowy musi zostać podłączony do jednego przełącznika rdzeniowego w każdej z dwóch serwerowni za pomocą linków 10G. W celu uniknięcia pętli w sieci należy zastosować mechanizm MLAG (lub równoważny). Niedopuszczalne jest stosowanie SpanningTree, EAPS, ERPS i innych mechanizmów ograniczających wykorzystanie pełnej przepustowości łącza.

Spanning tree musi zostać wyłączone na wszystkich portach i urządzeniach (również Rapid Spanning tree oraz Multiple spanning tree).

Na każdym z dostarczanych przełączników należy skonfigurować VLANy (w ilości zgodnej z potrzebami Partnera - minimum 30 VLANów). Nazwa każdego VLANu musi jednoznacznie wskazywać co najmniej TAG oraz przeznaczenie, adresację do zarządzania, konta administracyjne, NTP.

2.5. Konfiguracja oprogramowania do wykonywania kopii zapasowych

Należy zainstalować maszynę wirtualną dedykowaną dla wykonywanie backupu. Na serwerze Backup należy zainstalować Oprogramowanie Backup będące w posiadaniu Partnera Projektu, tj. Nakivo Backup & Replication oraz Veeam. Oprogramowanie należy skonfigurować, aby wykonywało Backup zgodny z harmonogramem tj.:

Systemy niezbędne do pracy szpitala (HIS):

- kopia przyrostowa co 12 godzin

- kopia pełna raz w tygodniu

- przechowywanie min. 1 kopii tygodniowej przez 4 tygodnie, 1 kopii miesięcznej przez 12 miesięcy, 7 ostatnich kopii przyrostowych

Systemy części szarej (ERP itp.):

- kopia przyrostowa co 24 godziny

- kopia pełna raz w tygodniu

- przechowywanie min. 1 kopii tygodniowej przez 4 tygodnie, 1 kopii miesięcznej przez 12 miesięcy, 7 ostatnich kopii przyrostowych

Inne systemy wspomagające pracę szpitala:

- kopia przyrostowa co 24 godziny od poniedziałku do piątku

- kopia pełna raz w tygodniu

- przechowywanie min. 1 kopii tygodniowej przez 4 tygodnie, 1 kopii miesięcznej przez 6 miesięcy, 3 ostatnie kopie przyrostowych

Systemy Archiwalne:

- kopia przyrostowa co 7 dni

- kopia pełna raz w miesiącu

- przechowywanie min. 1 kopii miesięcznej przez 6 miesięcy, 2 ostatnie kopie przyrostowych

Dyski w dostarczanym serwerze NAS należy skonfigurować w sposób zapewniający bezpieczeństwo danych, tj. RAID5. W celu udostępnienia zasobów dyskowych do serwera Backup należy skonfigurować LUN (lub LUNy). Komunikacja między serwerem a macierzą musi odbywać się po wydzielonej sieci logicznej (VLAN).

Polityka backupu i odtwarzania:

Wykonawca zobowiązany jest przygotować dokładną instrukcję opisującą sposób przygotowania kopii bezpieczeństwa oraz archiwizacji danych. Ponadto wykonawca winien przygotować instrukcję przywracania środowiska z kopii bezpieczeństwa.

Instrukcje powinny zawierać opis krok-po-kroku czynności niezbędnych do wykonania przy tworzeniu o odtwarzaniu backupu.

W celu zapewnienia poprawnego odtwarzania środowiska z kopii zapasowej, wykonawca winien zaprojektować procedurę testowego odtwarzania środowiska z kopii zapasowej. Testowe odtwarzanie nie powinno mieć wpływu na funkcjonujące środowisko produkcyjne.

2.6. Konfiguracja Active Directory

Wykonawca zobowiązany jest do uruchomienia usługi katalogowej MS Active Directory. Infrastruktura domenowa składać się musi z min. dwóch kontrolerów domeny.

Należy stworzyć użytkowników (około 500) (zgodnie z listą dostarczoną przez Partnera Projektu), grupy użytkowników, jednostki organizacyjne, polityki GPO, automatyczną instalację oprogramowania, skróty do aplikacji. Użytkowników należy dodać do grup zgodnie ze wskazówkami Partnera Projektu.

Dodatkowo należy przygotować plan dołączenia nowych oraz istniejących komputerów do domeny (minimum 300, maksymalnie 350 komputerów). Po uzgodnieniu z Partnerem Projektu dokładnego harmonogramu przełączenia komputerów do nowej domeny należy przeprowadzić operację przełączania w sposób minimalizujący przerwy w pracy. Całość operacji nie może trwać dłużej niż 24h. W ramach niniejszego zadania Wykonawca przygotuje i przekaże Partnerowi Projektu skrypt automatyzujący dodanie komputera do domeny.

Na osobnych maszynach wirtualnych należy zainstalować i skonfigurować:
- serwer plików
- serwer drukarek
- serwer aktualizacji

Na serwerze plików należy przygotować imienne foldery dla wszystkich użytkowników. Foldery powinny montować się automatycznie na komputerach po zalogowaniu użytkownika. Foldery powinny być widoczne jako dysk sieciowy.

Do folderów osobisty należy przenieść dane z obecnego serwera plików (ok. 3TB). Na serwerze plików należy utworzyć foldery współdzielone przez grupy użytkowników. Opis uprawnień do poszczególnych folderów zostaną dostarczone przez Partnera Projektu.

2.7. Instalacja UPSów w węzłach dystrybucyjnych

Dostarczone UPS 1500VA należy zainstalować we wszystkich szafach dystrybucyjnych (minimalnie 15, maksymalnie 18 sztuk) na terenie placówki. W przypadku gdy wymiary UPS nie pozwolą na instalację urządzenia w istniejącej szafie, Wykonawca zobowiązany jest do wymiany szafy oraz do przełożenia całej zawartości – w tym paneli krosowych. Termin wymiany oraz typ proponowanej szafy musi zostać skonsultowany i zaakceptowany przez Partnera Projektu.

3. Rozbudowa sieci strukturalnej

3.1. Zakres działań

Zakres działań dotyczy rozbudowy systemu okablowania w budynku przy ulicy Wolskiej 37, w niżej wskazanych strukturach sieci.

Wykonanie połączeń światłowodowych pomiędzy szafami teleinformatycznymi z wykorzystaniem kabli światłowodowych zewnętrznych SM 16J 9/125 odpornych na działanie szkodników (szczurów i innych gryzoni). Wydajność infrastruktury kablowej ma zapewnić parametry odpowiednie dla transmisji 100Gb/s.

3.2. Prace do wykonania – opis funkcjonalny

3.2.1. Relacje pomiędzy punktami dystrybucyjnymi

Pomiędzy punktami dystrybucyjnymi a serwerownią główną wymagane jest wykonanie połączenia światłowodowego 16j. Kable światłowodowe po obu stronach powinny zostać zakończone na panelu światłowodowym gniazdami LC. Pigtaile światłowodowe powinny zostać przyspawane do kabli światłowodowych. Zapas kabla pozostawiony w Szafie punktów dystrybucyjnych powinien pozwalać na powtórne wykonanie spawów. Zapas kabla pozostawionego w serwerowni powinien wynosić min. 10m.

Pomiędzy serwerowniami – główną oraz zapasową – wymagane jest wykonanie połączenia światłowodowego opartego o minimum 32 włókna światłowodu jednomodowego (dwa kable 16j). Kable światłowodowe po obu stronach powinny zostać zakończone na panelu światłowodowym gniazdami LC. Pigtaile światłowodowe powinny zostać przyspawane do kabli światłowodowych. Zapas kabla pozostawionego w serwerowni powinien wynosić min. 10m.

3.2.2. Wymagania techniczne

Okablowanie ma być prowadzone natynkowo w listwach osłonowych.

Informacja dotycząca tras kablowych znajduje w Załączniku nr 4 do Umowy.

Materiały użyte do realizacji zadania oraz stopień wykonania usługi mają odpowiadać normom aktywnym PL.

Wykonawca zobowiązany jest do przedłożenia stosownych dokumentów normujących wykonanie kompleksowego okablowania.

4. Dokumentacja powykonawcza

1. Dokumentacja powykonawcza musi zostać przygotowana w języku polskim oraz zawierać co najmniej:
    1) schemat i opis architektury logicznej i fizycznej rozwiązania wraz z wykazem komponentów użytych do budowy rozwiązania;
    2) raport z testów wykonanej rozbudowy sieci strukturalnej, infrastruktury teleinformatycznej po instalacji i konfiguracji dostarczonego Sprzętu i oprogramowania, w tym klastra przetwarzania danych, usługi katalogowej oraz poprawności działania trybu HA na skonfigurowanym Sprzęcie, przeprowadzonych na podstawie przygotowanych przez Wykonawcę scenariuszy testowych;
    3) dokumentację utrzymaniową administratora, w tym m.in. :
        a) sposób monitorowania infrastruktury,
        b) awarie:
            - diagnozowanie awarii,
            - opis najczęściej występujących problemów i awarii wraz z opisem procedur diagnostyczno-naprawczych,
            - instrukcję reagowania na ataki sieciowe typu DDOS, ARP itp.,
            - instrukcję odzyskiwania konfiguracji urządzeń w razie wystąpienia awarii.
        c) procedury administracyjne związane z bieżącą eksploatacją, w tym przełączania między serwerowniami,
        d) instrukcję dotycząca sposobów zbierania logów z dostarczonych urządzeń,
        e) harmonogram kopii zapasowych wraz z instrukcją przygotowywania kopii bezpieczeństwa, archiwizacji danych oraz przywracania środowiska z kopii bezpieczeństwa.
        f) politykę bezpieczeństwa wdrożonej infrastruktury,
    4) dokumentację instalacji, w tym dokumentację fotograficzną wykonanego montażu, uwzględniającą m.in.:
        a) wykaz i parametry dostarczonych elementów infrastruktury (sprzętu) wraz z numerami seryjnymi oraz miejscem instalacji,
        b) wykaz dostarczanego oprogramowania oraz licencji,
        c) schematy instalacji i wykonanych połączeń pomiędzy poszczególnymi elementami infrastruktury, w tym strukturę okablowania,
        d) charakterystykę i zakres funkcjonalny zainstalowanego oprogramowania.
    5) dokumentację konfiguracyjną, w tym zawartość plików i rejestrów konfiguracyjnych, skrypty startowe, architekturę logiczną i fizyczną, uwzględniającą wszystkie przeprowadzone prace m.in.:
        a) konfigurację połączeń sieciowych ,
        b) konfigurację ustawień dostarczonego Sprzętu,
        c) konfigurację interfejsów.
    6) kompletny wykaz kont wraz z hasłami wykorzystanych w konfiguracji elementów infrastruktury sprzętowej i programowej wraz z wyszczególnieniem lokalizacji oraz elementu, którego dotyczą te dane;
    7) szczegółowy opis integracji wszystkich elementów (zarówno sprzętowych jak i aplikacyjnych) oraz konfiguracji całego środowiska;
    8) kompletną adresację IP zamontowanych i skonfigurowanych urządzeń oraz zainstalowanego oprogramowania.

2. Dokumentacja, o której mowa w ust. 1, podlega akceptacji przez Partnera Projektu.
3. Dokumentacja o której mowa w ust. 1, musi zostać napisana w języku polskim, zgodnie z dokumentem „Zasady tworzenia dokumentacji projektowej" stanowiącym Załącznik nr 5 do Umowy.

5. Instruktaże dla Partnera Projektu

1. Wykonawca zobowiązany jest do przeprowadzenia instruktażu dla osób wskazanych przez Partnera Projektu w zakresie instalacji, konfiguracji, obsługi, utrzymania, monitoringu, zarządzania oraz administracji poniższym sprzętem oraz oprogramowaniem dostarczonym w ramach niniejszej Umowy, zgodnie z poniższym podziałem na bloki tematyczne:
    1) grupa I: przełączniki dostępowe, urządzenia firewall, serwer poczty elektronicznej, macierz do przechowywanie kopii zapasowych, serwer wirtualizacyjny (w tym System operacyjny oraz System wirtualizacji w zakresie min.: instalacja, administracja, konfiguracja wirtualizacji, konfiguracja maszyn wirtualnych, zarządzanie klastrem) – maksymalnie 2 osoby,
    2) grupa II: oprogramowanie do zarządzania dostępem do sieci, oprogramowanie do zarządzania zgłoszeniami – maksymalnie 2 osoby,
2. Zakres instruktażu musi obejmować także procedury reagowania na najczęściej występujące incydenty bezpieczeństwa oraz awarie w zakresie funkcjonalnym dostarczonych urządzeń i oprogramowania.
3. Przed rozpoczęciem instruktaży Wykonawca zobowiązany jest do przygotowania i przekazania uczestnikom agendy instruktaży oraz materiałów szkoleniowych w języku polskim w postaci papierowej i elektronicznej.
4. Instruktaż musi obejmować minimum 5 dni (po 6 godzin) dla każdej z grup uczestników.
5. Instruktaże odbędą się we wskazanych przez Partnera Projektu salach szkoleniowych na terenie Warszawy.
6. Zamawiający dopuszcza przeprowadzenie instruktarzy w formie on-line, o ile Partner Projektu wyrazi na to zgodę. Na czas przeprowadzenia instruktaży, Wykonawca udostępni Partnerowi Projektu platformę telekonferencyjną, która będzie umożliwiała połączenie audio-video uczestników z prowadzącym oraz opcję udostępniania pulpitu zdalnego uczestnikom w celu wyświetlenia prezentacji.
7. W ciągu jednego dnia może zostać przeprowadzony instruktaż tylko dla jednej grupy. Nie dopuszcza się prowadzenia równoległych instruktaży dla kilku grup w ciągu tego samego dnia.
8. Wykonawca przedstawi i uzgodni z Partnerem Projektu harmonogram przeprowadzenia instruktaży, na co najmniej 5 Dni Roboczych przed terminem ich rozpoczęcia.
9. Osoby prowadzące instruktaże muszą posiadać wystarczającą wiedzę i doświadczenie w zakresie technologii, której dotyczy instruktaż.