Załącznik nr 3 do SWZ

Opis przedmiotu zamówienia

Zakup i dostawa sprzętów i urządzeń na potrzeby modernizacji serwerowni w Urzędzie Miasta i Gminy w Rydzynie

1. Dostarczone urządzenia i sprzęty muszą być fabrycznie nowe, nieużywane, wolne od obciążeń i praw ustanowionych na rzecz osób trzecich.
   (Zamawiający dopuszcza, aby serwery w zadaniu 2 były nowe lub używane)
2. Jeżeli zapisy szczegółowe nie specyfikują inaczej, Zamawiający oczekuje prac w zakresie transportu i dostawy do urzędu oraz wniesienia wszystkich dostarczonych sprzętów i urządzeń.
3. Urządzenia muszą posiadać deklarację zgodności lub certyfikat CE.
4. Zamawiający wymaga dostarczenia dokumentu, o którym mowa w/w punkcie w postaci papierowej.
5. Dostarczony sprzęt musi zawierać licencje na każde oprogramowanie w postaci papierowej (lub naklejki producenta oprogramowania) oraz wszystkie informacje konieczne do zainstalowania tego oprogramowania (numery licencji, numery seryjne itp.).
6. Dyski twarde w przypadku uszkodzenia nie są zwracane do Wykonawcy. Weryfikacja uszkodzenia dysku odbywa się w siedzibie Zamawiającego.
7. Zamawiający musi mieć możliwość otwierania obudowy bez utraty gwarancji.
8. Przez usunięcie skutków awarii/wady rozumie się naprawę uszkodzonego Sprzętu. Usunięcie skutków awarii/wady obejmuje również uruchomienie oraz przetestowanie Sprzętu naprawionego lub Sprzętu zastępczego.
9. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
10. Serwis musi być realizowany przez producenta sprzętu lub autoryzowanego partnera serwisowego producenta (uprawniającego go do napraw gwarancyjnych urządzeń w imieniu producenta sprzętu).

Miejsce dostawy:
Dostawa urządzeń, sprzętu oraz oprogramowania w ramach niniejszego postępowania odbędzie się siedziby Urzędu Miasta i Gminy Rydzyna w budynku Gminy Rydzyna przy ul. Rynek 1 w Rydzynie.

Zadanie 1

1. Serwer 1 – 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 3,2 GHz każdy, dedykowany do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 135 pkt. w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Do oferty należy załączyć wydruk ze strony: www.spec.org potwierdzający spełnienie wymogów SWZ
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Obudowa	Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 24 dysków 2.5”. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
RAM	Minimum 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Zainstalowana w jednym slocie pamięć nie mniejsza niż 32GB Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Funkcjonalność pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	Min. 8 slotów PCIe generacji 4, w tym min. 1 sloty x16.

Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 wraz z wkładkami optycznymi w standardzie min. SFP+ odsługujące kable multimodowe, wkładki powinny obsługiwać falę o długości 850 nm, i mieć zasięg transmisji do min. 300 metrów, **kompatybilne z pozycją 4,5 zadania** (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 8 dysków SSD SAS o pojemności min. 1,9 GB, 12Gbps, 2,5“ Hot-Plug. Zamawiający wymaga dysków do zastosowań uniwersalnych, nie dopuszcza się dysków optymalizowanych tylko do odczytu lub tylko do zapisu. Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB skonfigurowane w RAID1 Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	5x USB, w tym min. 2 porty USB 3.0 1 porty VGA, Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 1400W każdy.
System operacyjny/ dodatkowe oprogramowani	Ze względu na wykorzystywane przez Zamawiającego środowisko Microsoft AD i potrzebę zachowania kompatybilności wymagany jest system operacyjny Microsoft Serwer 2022 Standard wraz z wieczystą licencją na wszystkie rdzenie procesora w oferowanym serwerze z możliwością uruchomienia 4 maszyn wirtualnych+ min 20 lic Cal na użytkownika. Wraz z serwerem Zamawiający wymaga dostarczenia bezterminowej licencji umożliwiającej stworzenie środowiska wirtualnego składającego się z min. trzech hostów (fizycznych serwerów) Zainstalowany obraz systemu witalizacyjnego na dyskach M.2 SATA **Oprogramowanie zapewniające zintegrowane bezpieczeństwo do zarządzenia infrastrukturą IT wraz z usługą wdrożenia opisane w punkcie 7 zadania** **Oprogramowanie do wykonywania kopii zapasowych opisane w punkcie 8 zadania**
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

	• zdalne monitorowanie i informowanie o statusie serwera (np. 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 WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE – załączyć do oferty. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows Server 2022
Warunki gwarancji	**Min. 2 lata gwarancji producenta**, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2. UPS – 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
na wejściu	
Zakres napięcia wejściowego w trybie podstawowym	140 – 280V
Częstotliwość wejściowa	50/60 Hz +/-3 Hz (automatyczne wykrywanie)
Typ gniazda wejściowego	BS1363A British, IEC 320 C20, Schuko CEE 7/EU1-16P
Długość przewodu zasilania	2,0 m.
Ilość kabli zasilających	1
na wyjściu	
Moc wyjściowa	2700W /3000 VA

Napięcie wyjściowe	230V
Zniekształcenia napięcia wyjściowego	Poniżej 5%
Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą)	50/60Hz +/- 3 Hz
Inne napięcia wyjściowe	208, 220, 240
Topologia	Line Interactive
Typ przebiegu	sinusoida
Złącza wyjściowe	(8) x IEC 320 C13 (Zasilanie zapasowe) (2) x IEC 320 C19 (Zasilanie zapasowe)
Akumulatory i czas podtrzymania	
Typ akumulatora	Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny
Typowy czas ładowania	3 godziny
Oczekiwana żywotność akumulatora (lata)	3-5 lat
Ilość zestawów RBC™	1
Możliwość podłączenia do 10 zewnętrznych modułów akumulatorowych	TAK
Akumulatory zewnętrzne typu plug-and-play	TAK
Akumulatory wymienialne przez użytkownika “na gorąco” bez przerywania pracy systemu	TAK
Czas podtrzymania przy obciążeniu 100% w trybie podstawowym	6 min 15sek
Czas podtrzymania przy obciążeniu 50% w trybie podstawowym	28 min 3sek
Efektywność urządzenia przy obciążeniu 100%	98,50%
Komunikacja i zarządzanie	
Interfejs Port (s)	RJ-45 Serial, SmartSlot
Moduł SNMP	Moduł WEB/SNMP obsługiwane protokoły komunikacyjne: IP v.6 SNMP v.3 HTTPS/SSL, SSH z kluczem do 2048 bit TLS wersja 1.2 SMTP, NTP, FTP, Telnet Modbus TCP Port uniwersalny do podłączenia np. czujnika temperatury (jeden czujnik temperatury dostarczyć w komplecie z UPS)
Panel sterowania	Wyświetlacz statusu LED ze wskaźnikiem pracy online: Zasilanie akumulatorowe: Wskaźniki Wymień baterię i Przeciążenie, Wielofunkcyjna konsola sterownicza i informacyjna LCD
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
Awaryjny wyłącznik zasilania (EPO)	TAK
Powiadomienie o rozłączeniu akumulatora	Powiadomienie o rozłączeniu akumulatora
Automatyczne włączenie UPS-a po powrocie zasilania	Automatycznie uruchamia podłączony sprzęt w momencie wznowienia zasilania z sieci miejskiej.
Ochrona przed przepięciami i filtracja	
Klasa energetyczna sprzętu przeciwprzepięciowego	645 Dżuli
Parametry fizyczne	
Maksymalna wysokość	432mm , 43,2cm
Maksymalna szerokość	178mm , 17,8cm
Maksymalna głębokość	483mm , 48,3cm
Wysokość w szafie	4U
Ciężar netto	38,64
Kolor	Czarny
Parametry środowiskowe	
Temperatura eksploatacji	0 – 40 °C

Wilgotność względna podczas pracy	0 – 95 %
Wysokość n.p.m. podczas pracy	0-3048 metrów
Temperatura (przechowywanie)	-15 – 45 °C
Wilgotność względna (przechowywanie)	0 – 95 %
Wysokość n.p.m. (przechowywanie)	0-15240 metrów
Hałas słyszalny w odległości 1 m od powierzchni urządzenia	55.0dBA
Rozpraszanie ciepła w trybie online	184.0 BTU/godz.
Klasa ochrony	IP 20
Certyfikaty i zgodność z normami	
Potwierdzenia zgodności	CE, CSA, EAC, EN 50091-1, EN 50091-2, EN/IEC 62040-1, EN/IEC 62040-2, FCC część 15 klasa A, IEC 60950, IRAM, RCM, VDE, WEEE
Okres gwarancji	2 lata gwarancji naprawy lub wymiany (bez akumulatora) i 1 lata na akumulator

3. Router i bramka bezpieczeństwa ze zintegrowanym przełącznikiem PoE i sieciowym rejestratorem wideo kompatybilny z pozycjami 1,2,4,5,6 z zadania – 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Procesor	4-rdzeniowy
Taktowanie procesora	1700 Mmz
Pamięć systemowa	4 GB DDR4
Pamięć wbudowana	16 GB eMMC Zintegrowany dysk 128 GB SSD
Zatoka HDD 3,5”	1
Przepustowość IDS/IPS	3.5 Gb/s (mierzona w iPerf3)
Maks. Pobór mocy (nie licząc wyjścia PoE)	50W
Sposób zasilania	1x Universalne wejście AC, 100-240VAC, 4.4A Maks, 50/60 Hz 1x USP-RPS wejście DC, 52VDC, 3.94A
Zasilanie	AC/DC, wewnętrzne, 240W
Obsługiwany zakres napięcia	100 do 240VAC
Interfejs zarządzania	Ethernet Bluetooth
Interfejs sieciowy	1x port WAN: 2.5 Gigabit Ethernet RJ45 8x portów LAN: 10/100/1000 Mb/s RJ45
Interfejs SFP+	1x WAN: 10G SFP+ 1x LAN: 10G SFP+
PoE	2x porty PoE+ IEEE 802.3at (pair A 1, 2+; 3, 6-) 6x portów PoE IEEE 802.3af (pair A 1, 2+; 3, 6-)
Maks. PoE na port 802.3af	15.4W
Maks. PoE na port 802.3at	30W
Zakres napięcia dla PoE 802.3af	44 do 57V
Zakres napięcia dla PoE 802.3at	50 do 57V
Zabezpieczenie ESD/EMP	Powietrze: +/- 15 kV, kontakt: +/- 8 kV
Przyciski	Reset
Certyfikaty	CE, FCC, IC
Wyświetlacz LCM	1x dotykowy ekran 1.3”
Wkładka SFP+	1 do połączenia LAN - odsługująca kable multimodowe, falę o długości 850 nm, i mieć zasięg transmisji do min. 300 metrów 1 do połączenia WAN - odsługująca kable multimodowe, falę o długości 850 nm, i mieć zasięg transmisji do min. 300 metrów
Uchwyt do montażu w szafie rack	w zestawie
Gwarancja	24 miesiące

4. Switch zarządzany SFP+ kompatybilny z pozycją 1,3,5 z zadania – 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Typ przełącznika	Zarządzany

Przełącznik wielowarstwowy	L2
Liczba zainstalowanych modułów	8 x 1/10G SFP+
Przepustowość rutowania / przełączania	160 Gbit/s
Wydajność	80 Gbit/s
Prędkość przekazywania	119,04 Mpps
Typ obudowy max	1U Rack
Maksymalne zużycie mocy	30 W
Certyfikaty	CE, FCC, IC
Okablowanie	W zestawie Patchord multimodowy SFP+ 10G do podłączenia z: - 1 urządzeniem z pozycją 1 z zadania o długości 2m – 2 szt. - 1 urządzeniem z pozycją 3 z zadania o długości 2m – 2 szt. - 1 urządzeniem z pozycją 5 z zadania o długości 2m – 2 szt. - 1 urządzeniem z pozycją 5 z zadania o długości 3m – 2 szt. - 2 serwerami za zadania 2 o długości 3m – 4 szt
Wkładka SFP+	min 6 szt - odsługująca kable multimodowe, falę o długości 850 nm, i mieć zasięg transmisji do min. 300 metrów
Uchwyt do montażu w szafie rack	w zestawie
Gwarancja	24 miesiące

5. Switch zarządzany kompatybilny z pozycją 1,2,3 z zadania – 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Typ przełącznika	Zarządzany
Przełącznik wielowarstwowy	L2/L3
Liczba portów Ethernet (10/100/1000)	48
Liczba zainstalowanych modułów SFP+	4
Standardy komunikacyjne	IEEE 802.1x
Obsługa 10G	Tak
Dublowanie portów	Tak
Podpora kontroli przepływu	Tak
Agregator połączenia	Tak
Kontrola wzrostu natężenia ruchu	Tak
Protokół drzewa rozpinającego	Tak
Obsługa sieci VLAN	Tak
Przepustowość rutowania / przełączania	176 Gbit/s
Prędkość przekazywania	130,944 Mpps
Typ uwierzytelniania	IEEE 802.1x,RADIUS
Maksymalne zużycie mocy	60 W
Obsługa PoE	Nie
Certyfikaty	CE, FCC, IC ETSI300-019-1.4
Wkładka SFP+	min 2 szt - odsługująca kable multimodowe, falę o długości 850nm, i mieć zasięg transmisji do min. 300 metrów
Uchwyt do montażu w szafie rack	w zestawie
Gwarancja	24 miesiące

6. Punkt dostępowy kompatybilny z pozycją 3 z zadania – 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Interfejsy sieciowe	2 gigabitowe porty Ethernet 10/100/1000
Przyciski	Reset
Anteny	3 anteny o podwójnej polaryzacji i zysku 3 dBi
Standardy WiFi	802.11 a/b/g/n/ac
Tryby POE	802.3af 802.3at PoE+
Sposób zasilania	Pasywne PoE (48 V), 802.3af/803.2at Zakres napięcia: 44 - 57 V DC
Zasilacz	48 V, 0.5 A gigabitowe PoE (w zestawie)
Maksymalny pobór mocy	9 W
Moc nadawcza	2.4 GHz: min 22 dBm 5 GHz: min 22 dBm

BSSID	4 na radio
Oszczędzanie energii	Wspierane
Zabezpieczenia	WEP, WPA-PSK, WPA-Enterprise (WPA / WPA2, TKIP / AES)
Certyfikaty	CE, FCC, iC
Montowanie	Na suficie / ścianie (uchwyty w zestawie)
Dopuszczalna temperatura pracy	Od -10 do 70 st. C
Dopuszczalna wilgotność	5%-95% niekondensująca
Zaawansowane zarządzanie ruchem	
VLAN	802.1Q
QoS	Limit ustawiany na użytkownika
Izolowanie ruchu gości	Wspierane
WMM	Voice, Video, Best Effort, Background
Jednocześni klienci	200
Wspierane przepustowości (zależnie od modulacji / szerokości kanału)	
Standard	Przepustowość
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mb/s
802.11n	6,5 - 450 Mb/s (MCS0 - MCS23, HT 20/40)
802.11ac	6,5 - 1300 Mb/s (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
802.11b	1, 2, 5.5, 11 Mb/s
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mb/s
Gwarancja	24 miesiące

7 Oprogramowanie zapewniające zintegrowane bezpieczeństwo do zarządzenia infrastrukturą IT wraz z usługą wdrożenia /*lub równoważny*

I. **Wymagania licencyjne:**

1. Program będzie dostarczony na licencji bezterminowej, która umożliwia na pełne wykorzystanie oprogramowania bez granicznej daty użytkownika.
2. Program będzie zapewniał możliwość pracy nielimitowanej liczbie administratorów oraz osób odpowiedzialnych za realizację zadań pomocy technicznej.
3. **Program będzie zapewniał obsługę minimum 60 stacji roboczych Windows z użyciem agenta.**
4. **Wsparcie producenta rozwiązania będzie ważne przez min. 12 miesięcy licząc od daty dostawy oraz podpisania przez Strony protokołu odbioru zdawczo-odbiorczego bez uwag, w zależności od tego, która czynność przypadnie później.**

II. **Wymagania ogólne:**

1. Zamawiający wymaga dostarczenia oprogramowania posiadającego budowę modułową, składającego się z serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami będzie nawiązywana przy użyciu szyfrowanego protokołu TLS w wersji 1.2 lub wyższej.
3. Moduły po będzie umożliwiał kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.
4. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., będą odseparowane od danych technicznych. Będą również grupowane w osobnym, dedykowanym oknie. Powinno pozwalać to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
5. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, będzie objęty kontrolą na poziomie wybranych Administratorów – w programie będzie możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator będzie miał możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. powinien mieć możliwość wyłączenia zdalnej deinstalacji Agenta, ograniczenia dostępu do Opcji programu oraz logów działań innych administratorów
6. Działania administratorów będą logowane, oznacza to, że program będzie posiadał dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów będą automatycznie eksportowane do zewnętrznego kolektora Syslog.

7. Jeżeli oferowane oprogramowanie/system wymaga odrębnych licencji (systemu operacyjnego lub bazodanowego lub działa na licencjonowanym systemie operacyjnym, lub licencjonowane są komponenty wchodzące w skład infrastruktury Zamawiającego, lub licencjonowana jest ilość użytkowników, serwisantów/administratorów) Zamawiający wymaga dostarczenia niezbędnych licencji.
8. Program będzie zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
9. Agent w procesie instalacji ręcznej będzie posiadał możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
10. Oprogramowanie będzie posiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, prezentującymi dane ze wszystkich modułów funkcjonalnych oprogramowania:
    1) Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
    2) Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
    3) Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW,
    4) Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
    5) Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem)

III. **Wymagania dla funkcjonalności monitorowania infrastruktury obejmującej serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle:**

1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping.
2. Wykrywanie urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU).
3. Wizualizacja stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci.
4. Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z możliwością wyboru koloru tła.
5. Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
6. Wizualizacji map urządzeń poprzez grupowanie urządzeń i przedstawianie ich za pomocą kształtu graficznego.
7. Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
8. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
9. Zablokowanie mapy urządzeń przed przypadkową edycją.
10. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów.
11. Serwer pocztowy:
    a. monitorowanie czasu logowania do serwisu odbierającego oraz czasu wysyłania poczty;
    b. możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem);
    c. możliwość wykonywania operacji testowych;
    d. możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
12. Monitorowanie serwerów WWW i adresów URL.
13. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.
14. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail.
15. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.
16. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
17. Monitoring routerów i przełączników wg:
    a) zmian stanu interfejsów sieciowych;
    b) ruchu sieciowego;
    c) podłączonych stacji roboczych – graficzna prezentacja panelu switcha;
    d) ruchu generowanego przez podłączone do portów stacje robocze.

18. Serwis Windows: monitor serwisów Windows powinien alarmować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie.
19. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.
20. Wydajność systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
21. Kompilacja plików MIB, umożliwiająca dodawanie definicji dla modułów SNMP.
22. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów.
23. Definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera.
24. Budowanie alarmów przez administratora z wykorzystaniem ciągu przyczynowo skutkowego (możliwość samodzielnego wskazania przez administratora dowolnego zdarzenia z listy, którego wykrycie wzbudzi alarm oraz dowolnej liczby akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie).
25. Integracja ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

IV. **Wymagania dla funkcjonalności inwentaryzacji:**

1. Automatycznie gromadzenie informacje o sprzęcie i oprogramowaniu na stacjach roboczych.
2. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
3. Prezentacja zestawień posiadanych konfiguracji sprzętowych, wolnego miejsca na dyskach, średniego wykorzystanie pamięci, informacji pozwalających na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informowanie o zainstalowanych aplikacjach oraz aktualizacjach Windows (możliwość audytowania i weryfikacji użytkowania licencji.
5. Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itp.
6. Wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Możliwość odczytania numeru seryjnego (klucze licencyjne).
8. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Tworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Wymiana plików „do” i „ze” stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane.
12. Tworzenie powiązań między zasobami a urządzeniami.
13. Tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych.
14. Wskazywanie osób uprawnionych do użycia zasobów.
15. Definiowanie własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania z możliwością dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (data, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz
16. Określenie atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów.
17. Określenie atrybutów dodatkowych tylko dla wybranych typów zasobów.
18. Definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie.
19. Import danych z zewnętrznego źródła (.CSV).
20. Przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.
21. Tworzenie powiązań między zasobami a dokumentami.

22. Oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.
23. Ewidencja czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności.
24. Generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania;
25. Przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo Zamawiającego.
26. Konfiguracja stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca.
27. Konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca.
28. Archiwizacja i porównywanie audytów zasobów.
29. Tworzenia kodów kreskowych dla zasobów.
30. Drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy.
31. Inwentaryzacja zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet.
32. Inwentaryzacja stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline).
33. Definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).
34. Agent inwentaryzacji na system Android który powinien zapewniać funkcjonalność pozyskiwania informacji o oprogramowaniu i audycie licencji w zakresie:
    a) Skanowania plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
    b) Informacji o aplikacjach używanych u Zamawiającego;
    c) Tworzenia własnych wzorców aplikacji;
    d) Tworzenia dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
    e) Informacji o komputerach, na których aplikacja została wykryta;
    f) Zarządzania posiadanymi licencjami;
    g) Wskazywania osób odpowiedzialnych za licencję;
    h) Wskazania użytkowników licencji;
    i) Tworzenia powiązań między licencjami a dokumentami;
    j) Zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu;
    k) Audyt legalności oprogramowania oraz powiadomień w razie przekroczenia liczby posiadanych licencji - z możliwością wykonania aktualnych raportów audytowych;
    l) Raport zgodności licencji;
    m) Możliwości przypisania do programów numerów seryjnych, wartości itp.

v. **Wymagania dla funkcjonalności obsługi użytkowników:**
1. Monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows.
2. Monitorowanie faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).
3. Monitorowanie procesów (każdy proces powinien mieć możliwość podania całkowitego czasu działania oraz czasu aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach.
4. Monitorowanie rzeczywistego użytkowania programów (m.in. procentowej wartoś wykorzystania aplikacji, obrazującej czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność.
5. Monitorowanie informacji o edytowanych przez użytkownika dokumentach.
6. Monitorowanie historii pracy (cykliczne zrzuty ekranowe).
7. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt).
8. Monitorowanie transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika).
9. Monitorowanie wydruków m.in. przekazywania informacji o dacie wydruku, informacji o wykorzystaniu drukarek, raportów dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na

jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Monitorowanie kosztów wydruków.
10. Monitorowanie nagłówków przesyłanej w aplikacjach Zamawiającego poczty e-mail.
11. Blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
12. Blokowanie ruchu na wskazanych portach TCP/IP
13. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem.
14. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia.
15. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika).
16. Definiowanie godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
17. Generowanie raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
18. Blokowanie uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i powinny być kopiowane pomiędzy grupami lub kontami.
19. Możliwość uzyskania dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w Szpitalu, za pomocą funkcji zdalnego dostępu przez każdego pracownika

VI. Wymagania dla funkcjonalności ochrony danych przed wyciekiem:

1. Możliwość blokowania urządzeń i nośników danych.
2. Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
3. Możliwość blokowania urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek.
4. Możliwość blokowania interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
5. Możliwość blokownia tylko urządzeń służących do przenoszenia danych (inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane).
6. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
7. Wsparcie bezpieczeństwa systemu:
   a) integracja i zarządzanie ustawieniami Windows Defender;
   b) integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu;
   c) monitorowanie stanu szyfrowania dysków BitLocker;
   d) monitorowanie stanu modułu TPM.
8. Zarządzanie prawami dostępu do urządzeń:
   a) możliwość definiowania praw użytkowników/grup do odczytu, zapisu czy wykonania plików;
   b) możliwość autoryzowania urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane;
   c) możliwość całkowitego zablokowania określonych typów urządzeń dla wybranych użytkowników;
   d) możliwość całkowitego zablokowania określonych typów urządzeń dla wybranych użytkowników;
   e) możliwość usuwania z listy znanych urządzeń nośników, które np. zostały zutylizowane.
9. Audyt operacji na plikach na urządzeniach przenośnych:
   a) zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych;
   b) podłączenie/odłączenie urządzenia przenośnego.
10. Możliwość monitorowania operacji na plikach w lokalnych folderach komputera użytkownika.
11. Możliwość integracji z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Możliwość przydzielania uprawnień do kont użytkowników lokalnych.

VII. Wymagania dla funkcjonalności realizacji zdalnej pomocy użytkownikom, poprzez:

1. podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla);

2. zablokowanie w trakcie zdalnego dostępu działania myszy oraz klawiatury dla użytkownika;
3. zdefiniowanie bazy zgłoszeń umożliwiającej użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom/serwisantom, otrzymującym automatycznie powiadomienie o przypisanym im problemie;
4. możliwość przetwarzania zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz posiadanie dokumentów prawnych dot. ochrony sygnalistów w tym szablonów regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
5. umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem/serwisantem poprzez komentarze, które są wpisywane i widoczne dla obu stron;
6. wbudowany komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami/serwisantami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy;
7. umożliwienie informowania pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy;
8. dedykowany portal w oparciu o przeglądarkę internetową, który jest dostępem do systemu zgłoszeń oraz bazy wiedzy,
9. pobieranie listy użytkowników z Active Directory;
10. zarządzania lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont;
11. zarządzanie dostępem Administratorów/Serwisantów do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń;
12. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej;
13. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO;
14. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników;
15. procesowanie zgłoszeń użytkowników z wiadomości e-mail;
16. wykonywanie operacji na wielu zgłoszeniach równocześnie;
17. dołączanie załączników do zgłoszeń;
18. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników;
19. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia;
20. dystrybucję oprogramowania przez Agenta;
21. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI);
22. zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji powinno następować kolejkowanie zadania dystrybucji pliku;
23. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych użytkowników w zgłoszeniu;
24. planowanie nieobecności Administratorów/Serwisantów;
25. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem;
26. generowanie raportów obsługi helpdesk;
27. zarządzanie procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami);
28. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

VIII. Wymagania dla prac wdrożeniowo-szkoleniowych:

1. Zakres minimalnych prac w obszarze przeprowadzenia szkolenia dla pracowników Działu Informatyki Zamawiającego pełniącego rolę pracownika pomocy technicznej wdrażanego systemu:
   a. Zakres szkolenia:
      a) Ogólne omówienie rozwiązania i jego struktury;
      b) Praca w obszarze obsługi zgłoszeń w przypadku pełnienia roli osoby obsługującej zgłoszenie;
      c) Praca w obszarze obsługi zgłoszeń w przypadku pełnienia roli osoby obserwującej zgłoszenie;
      d) Praca w obszarze obsługi zgłoszeń w przypadku pełnienia roli osoby zgłaszającej problem czy potrzebę;
      e) Możliwości pomocy zdalnej i komunikacji ze zgłaszającym;
      f) Mechanizmy raportowania i generowania statystyk w zgłoszeniach;

g) Rozwiązywanie najczęstszych problemów;
h) Egzamin certyfikujący.

b. Czas trwania szkolenia:
a) Minimum 5 godziny dla pracowników Działu Informatyki odpowiedzialnych za obsługę systemu zgłoszeń;
b) Szkolenie powinno się kończyć egzaminem oraz wydaniem certyfikatu.

Prace wdrożeniowo-szkoleniowe powinny być przeprowadzone przez inżyniera certyfikowanego przez producenta oferowanego rozwiązania.

8 Oprogramowanie do wykonywania kopii zapasowych.

I. Wymagania licencyjne
1. Oprogramowanie będzie zapewniać obsługę minimum 15 obciążeń (maszyn wirtualnych, fizycznych)
2. Wsparcie producenta rozwiązania będzie uprawniać do wykonywania aktualizacji i przejścia na nową wersję przez okres min. 60 miesięcy
3. Oprogramowanie będzie można rozszerzyć do minimum 50 obciążeń (maszyn wirtualnych, fizycznych)

II. Wymagania ogólne
1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

III. Całkowite koszty posiadania
1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
4. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
5. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
6. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
7. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.

10. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
11. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
12. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
13. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
14. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
15. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
16. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

IV. Wymagania RPO

1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2. Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
4. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
5. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
6. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
7. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
8. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
9. Oprogramowanie musi posiadać wsparcie dla NDMP
10. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
11. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
12. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
13. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
14. Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
15. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
16. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
17. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być

możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
18. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
19. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
20. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

v. Wymagania RTO
1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
7. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
8. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
9. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
   - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
   - BSD: UFS, UFS2
   - Solaris: ZFS, UFS
   - Mac: HFS, HFS+
   - Windows: NTFS, FAT, FAT32, ReFS
   - Novell OES: NSS
10. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
11. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
12. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
13. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
15. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
17. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
18. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
19. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
20. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
21. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA

24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

VI. Ograniczenie ryzyka

1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
4. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
5. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
6. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

VII. Monitoring

1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4. System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware
5. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
6. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
7. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
8. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
9. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
10. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
11. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
12. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
13. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
14. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
15. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
16. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
17. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

18. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x

VIII. Raportowanie

1. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019
2. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
3. System musi być certyfikowany przez VMware i posiadać status „VMware Ready"
4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
11. System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Zadanie 2

1. Serwer – 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Procesor	2xCPU Warunki użytkowania Server/Enterprise Bazowa częstotliwość procesora: 2.30 GHz Maks. częstotliwość turbo: 3.10 GHz Liczba rdzeni na procesor: 12 Liczba wątków procesor: 24 Pamięć Cache: 30 MB Liczba linków QPI: 2 Wielkość pamięci obsługiwanej przez procesor: 768 GB Znamionowa moc termiczna procesora nie większa niż 150W Obsługa pamięci ECC Liczba kanałów pamięci 4 Procesor po raz pierwszy wprowadzony na rynek nie wcześniej niż 3 kwartał 2014 rok Procesor zaprojektowany do pracy w serwerach umożliwiające osiągnięcie wyniku: minimum 22000 punktów w teście dostępnym na stronie internetowej www.cpubenchmark.net dla konfiguracji Multiple CPU

	Do oferty należy załączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów SWZ (wynik od publikacji ogłoszenia do dnia składnia ofert).
Chipset	Płyta główna z możliwością zainstalowania do dwóch procesorów Intel. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Obudowa	Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 8 dysków 3.5". Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Pamięć RAM	Minimum 256GB DDR4 RDIMM 2133MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Zainstalowana w jednym slocie pamięć nie mniejsza niż 32GB Płyta główna powinna obsługiwać do 1,5TB pamięci RAM.
Dysk twardy	minimum 8 wnęk dla dysków twardych Hotplug 3,5" W zestawie kieszenie do dysków do wszystkich wnęk.
Kontrolery RAID	Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Obsługa dysków o min pojemności 10 TB Obsługa dysków SAS: o prędkości 12Gbit i SATA: o prędkości 6Gbit
Połączenia i karty sieciowe	Wbudowane min. 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w min. w standardzie SFP+ wraz z wkładkami optycznymi w standardzie min. SFP+ odsługujące kable multimodowe, wkładki powinny obsługiwać falę o długości 850 nm, i mieć zasięg transmisji do min. 300 metrów, (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Kompatybilne z Ubquity Unifi
Wbudowane porty	- Zintegrowana karta graficzna ze złączem VGA; - min 1x USB 2.0 dostępne na froncie obudowy - min 2x USB 3.0 dostępne z tyłu serwera - min 1x USB 3.0 wewnątrz serwera - Możliwość instalacji dodatkowego portu VGA wyprowadzonego z przodu obudowy serwera; Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; - Moduł SD
Wentylatory	Redundantne
Zasilacz	Redundantne, Hot-Plug min. 750W każdy
Diagnostyka	Wbudowane diody informacyjne lub wyświetlacz informujący o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, status karty zarządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • 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 WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory;

	• możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Gwarancja	**Min. 24 miesięcy gwarancji**. Wymagane jest oświadczenie wykonawcy lub producenta sprzętu o spełnieniu tego warunku – dostarczenie dokumentu na wezwanie Zamawiającego A) Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie wykonawcy (lub jego przedstawiciela w Polsce) potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta (oświadczenie dostarczane na wezwanie Zamawiającego). B) Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera. Oświadczenie wykonawcy (lub jego przedstawiciela w Polsce) dostarczane na wezwanie Zamawiającego. Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001 – dokument potwierdzający, że serwis urządzeń będzie realizowany zgodnie z tą normą - dostarczane na wezwanie Zamawiającego Wymagane okno czasowe dla zgłaszania usterek min wszystkie dni robocze w godzinach od 8:00 do 17:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne.
Certyfikaty i standardy	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE – dołączyć do oferty.
Wsparcie techniczne producenta	A) Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera B) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. C) W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane.
Wspieranie OS:	- Windows Server 2016, - Windows Server 2016 Hyper-V, - VMware ESXi 7.0 U3, - VMware ESXi 8.0;

2. Dysk do serwera – 16 sztuk – nowe

Parametr	Charakterystyka (wymagania minimalne)
Dedykowany do	serwery
Rodzaj dysku	wewnętrzny
Typ	HDD (magnetyczny)
Format	3.5 cala
Interfejs	Serial ATA III
Pojemność	10 TB
Prędkość obrotowa	7200 obr./min.
Pamięć cache	256 MB
Szybkość transmisji interfejsu dysku twardego	6 Gbit/s
Transfer zewnętrzny	270 MB/s
Wytrzymałość na wstrząsy w czasie pracy	50 G
Niezawodność MTBF	2000000 godz.
Gwarancja producenta	36 miesiące

Dysk kompatybilny z serwerami z zadania 2

3. Dysk kopii zapasowych – 2 sztuk – nowe

Parametr	Charakterystyka (wymagania minimalne)
Dedykowany do	serwery
Rodzaj dysku	wewnętrzny
Typ	HDD (magnetyczny)
Format	3.5 cala
Interfejs	Serial ATA III
Pojemność	16 TB
Prędkość obrotowa	7200 obr./min.
Pamięć cache	512 MB
Szybkość transmisji interfejsu dysku twardego	6 Gbit/s
Transfer zewnętrzny	260 MB/s
Wytrzymałość na wstrząsy w czasie pracy	50 G
Niezawodność MTBF	2500000 godz.
Gwarancja producenta	36 miesiące

Dysk kompatybilny ze stacją dokującą z zadania 2

4. Stacja dokująca na dwa dyski

Parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	Zewnętrzna
Rozmiar	2,5"/3,5"
Interfejs obudowy	USB 3.1
Interfejs dysku	SATA minimum do 16 TB
Transfer zapisu dla USB 3.1	10000 Mbps
Dodatkowe informacje	Hot Plug, Plug & Play, Dioda LED informująca o pracy urządzenia
Dołączone akcesoria	Zasilacz sieciowy, Kabel USB
Gwarancja	24 miesiące