Załącznik nr 2 SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest realizacja założeń projektu Cyfrowa Gmina realizowane w ramach umowy o powierzenie grantu o numerze 3343/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

2. Zamówienie podzielone na następujące części:

Cześć I - Sprzęt komputerowy z oprogramowaniem

I. Stacja robocza AiO – 27 szt.

Nazwa	Wymagane minimalne parametry techniczne	
Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora.	
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna	
Wydajność obliczeniowa	Komputer w oferowanej konfiguracji musi osiągać w teście wydajnościowym BAPCO wynik SYSmark 25 Overall Rating – 1100 punktów Dokumentem potwierdzającym spełnianie ww. wymagań będzie wydruk raportu z oprogramowania testującego, potwierdzony za zgodność z oryginałem przez Wykonawcę – **załączyć na wezwanie Zamawiającego** Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). **Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego**	
Pamięć RAM	16 GB DDR4 2666MHz możliwość rozbudowy do 32GB RAM.	
Pamięć masowa	256GB SSD M.2 NVMe Możliwość instalacji dodatkowego dysku twardego M.2 lub 2.5	
Grafika	Musi umożliwiać pracę dwumonitorową; Karta osiągająca w teście PassMark Video card wynik 1500 punktów według wyników ze strony https://www.videocardbenchmark.net	
Matryca	Rozmiar matrycy / plamki	23,8” / max. 0,275mm
	Rozdzielczość	FHD (1920x1080)
	Jasność typowa	250 cd/m²
	Kontrast typowy	600:1
	Kąty widzenia poziom/pion	178/178
	Rodzaj matrycy	Matowa IPS
Wyposażenie	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki 2W	

multimedialne	na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 1.0 MP z diodą LED informującą użytkownika o pracy, Mechaniczna, chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy) Wbudowane w obudowę dwa mikrofony
Obudowa	Typu All-in-One zintegrowana z monitorem 23.8 cali. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Zasilacz o mocy 65W o efektywności 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności 80% przy obciążeniu zasilacza na poziomie 100%, Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa musi umożliwiać regulację pochyłu pionowego w zakresie od -5 do 30 stopni.
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: - Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; - Zdalną konfigurację ustawień BIOS
Bezpieczeństwo	Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy

	rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Wymagane informacje z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach), procesor (typ, nazwa, prędkość, cache L2 i L3), pojemności zainstalowanych dysków twardych, MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje muszą być dostępne w menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne] - użytkownika/systemowego - hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywanie zmian ustawień BIOS, rozruch systemu operacyjnego - hasło blokuje start systemu operacyjnego. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA, kontrolera audio, układu TPM, wbudowanej kamery i czytnika kart multimedialnych, czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. Możliwość zdefiniowania automatycznego uruchamiania komputera codziennie lub w wybrane dni tygodnia, Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Komputer musi być wyprodukowany zgodnie z normą ISO9001 i ISO 5001 – certyfikaty dla producenta sprzętu **załączyć na wezwanie zamawiającego;** Certyfikat ISO 50001 dla producenta sprzętu **- załączyć na wezwanie zamawiającego;** Oświadczenie producenta sprzętu, że oferowany sprzęt pochodzi z autoryzowanego kanału sprzedaży na rynek UE **– załączyć na wezwanie zamawiającego**
Porty/ złącza	Wbudowane porty: 1x HDMI 1x USB 2.0 3x USB 3.2 Typ-A Nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości

	1x audio jack 1x RJ-45 port 10/100/1000 Mbps Czytnik kart SD Karta WiFi ac+ bluetooth 5.1 Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki musi być; wyposażona w: 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, 1 złącze M.2 dla dysku twardego oraz 1 złącze M.2 dla karty WiFi. Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez

	konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: **a)** Login i hasło, **b)** Karty inteligentne i certyfikaty (smartcard), **c)** Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 45. Umożliwiający pracę w domenie;

Oprogramowanie użytkowe	Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - upgrade i instalację wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość sprawdzenia przed instalacją każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta, a w szczególności informacji : a) poprawkach i usprawnieniach dotyczących aktualizacji b) dacie wydania ostatniej aktualizacji c) priorytecie aktualizacji d) zgodności z systemami operacyjnymi e) jakiego komponentu sprzętu dotyczy aktualizacja f) wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika lub aplikacji; - rozpoznawanie modelu oferowanego komputera, w tym numeru seryjnego komputera; - sprawdzenie historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą i wersją - wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością export; - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych, ściągniętych, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów dotyczyły, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu; Raport musi zawierać dokładną datę i godzinę z podjętych i wykonanych akcji/zadań;
Warunki gwarancji, wsparcie techniczne	3-letnia gwarancja z czasem reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego; Wykonawca musi posiadać ISO 9001 i ISO 27001 na świadczenie usług serwisowych – **okazać na wezwanie Zamawiającego;** Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta, w tym: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego;

II. Serwer Typ I z oprogramowaniem – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Typu RACK, wysokość maksymalnie 2U; Szyny umożliwiające wysunięcie serwera z szafy stelażowej; Ramię porządkujące ułożenie przewodów z tyłu serwera; Możliwość zainstalowania 8 dysków twardych hot plug; Możliwość rozbudowy do 24 slotów na dyski; Zainstalowane: 3 dyski SSD 960GB, 1 dysk SSD 1,92TB, 2 dyski 2,4TB SAS 10k rpm; Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray; Możliwość zainstalowania dedykowanego wewnętrznego napędu taśmowego w technologii LTO;
Płyta główna	1. Dwuprocesorowa; 2. Wyprodukowana i zaprojektowana przez producenta serwera 3. Możliwość instalacji procesorów 28-rdzeniowych; 4. Zainstalowany moduł TPM 2.0 5. 6 złącz PCI Express generacji 3 w tym: • 3 fizyczne złącza o prędkości x16; • 3 fizyczne złącza o prędkości x8; • Możliwość rozbudowy o dodatkowe 2 złącza pełnej wysokości; 6. 24 gniazda pamięci RAM; 7. Obsługa minimum 3TB pamięci RAM; 8. Wsparcie dla technologii: • Memory Scrubbing • SDDC • Advanced ECC • Rank Sparing; 9. Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM o pojemności sumarycznej minimum 1TB. Przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan w przypadku nagłej awarii zasilania. Nie dopuszcza się podtrzymania bateryjnego stanu pamięci; 10. 2 sloty dla dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express nie zajmujące klatek dla dysków hot-plug;
Procesor	Osiągający w teście PassMark CPU Mark 20200 - wydruk ze strony https://www.cpubenchmark.net lub www.passmark.com – **załączyć na wezwanie Zamawiającego**
Pamięć RAM	64 GB pamięci RAM DDR4 Registered 2933Mhz

Interfejsy LAN	Nie zajmujące slotów PCI Express, 6 x 1Gbit Base-T;
Kontrolery I/O	Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50
Porty	Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; 1x zewnętrzny port USB; 2 x USB 3.0 z przodu i 2 x USB 3.0 z tyłu; Port serial, możliwość wykorzystania portu serial do zarządzania serwerem; Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
Zasilanie, chłodzenie	Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy 800W; Redundantne wentylatory hotplug;
Zarządzanie	1. Wbudowane diody lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii 2. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: • karty rozszerzeń zainstalowanej w dowolnym slocie PCI Express • CPU • pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM • wbudowanego na płycie głównej nośnika pamięci M.2 SSD • karty zrządzającej serwera • wentylatorów • baterii podtrzymującej ustawienia BIOS płyty głównej • zasilaczy 3. System przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia zasilania serwera; 4. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, umożliwiający pełne zarządzanie i zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s i złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web, SSH; • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; • Zarządzanie alarmami poprzez SNMP; • Możliwość przejęcia konsoli tekstowej

	• Możliwość zarządzania przez kilku administratorów jednocześnie • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Obsługa serwerów proxy (autentykacja) • Obsługa VLAN • Możliwość konfiguracji parametru Max. Transmission Unit (MTU) • Wsparcie dla protokołu SSDP • Obsługa protokołów TLS 1.2, SSL v3 • Obsługa protokołu LDAP • Synchronizacja czasu poprzez protokół NTP • Możliwość backupu i odtworzenia ustawień BIOS serwera oraz ustawień karty zarządzającej 5. Oprogramowanie zarządzające i diagnostyczne producenta serwera, umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii; 6. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez używania zewnętrznych nośników lub kopiowania danych przez sieć LAN; 7. Możliwość konfiguracji i aktualizacji BIOS, firmware, sterowników bezpośrednio z GUI karty zarządzającej serwera bez pośrednictwa innych nośników poza obrębem karty zarządzającej.
Gwarancja	3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; Wykonawca musi posiadać ISO 9001 i 27001 na świadczenie usług serwisowych – **okazać na wezwanie Zamawiającego;** Bezpłatna dostępność poprawek i aktualizacji BIOS/firmware/sterowników dożywotnio dla oferowanego serwera;
Dokumentacja, inne	Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – **oświadczenie producenta załączyć na wezwanie zamawiającego;** Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – **oświadczenie producenta załączyć na wezwanie zamawiającego;**

	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; W czasie obowiązywania gwarancji na sprzęt, po podaniu na infolinii numeru seryjnego urządzenia , możliwość weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
System operacyjny	Licencja musi uprawniać do zainstalowania w środowisku fizycznym lub dwóch instancji wirtualnych; Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Dodawanie i wymiana pamięci RAM bez przerywania pracy. 6) Dodawanie i wymiana procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

	d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu; 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dwadzieścia licencji dostępowych dla użytkowników sieciowych; 23) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 24) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach; 25) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 26) Możliwość implementacji następujących funkcjonalności bez potrzeby

	instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych; c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach; m) 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. n) Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 27) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek; 29) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 30) Mechanizmy zdalnej administracji oraz mechanizmy administracji przez skrypty. 31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

III. Serwer Typ II z oprogramowaniem – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Typu TOWER; Opcjonalna możliwość konwersji do RACK 4U; Możliwość zainstalowania 8 dysków twardych hot plug 2,5”; Zainstalowane 3 dyski SSD o pojemności 960GB Mixed-use Zainstalowany jeden dysk SSD o pojemności 1,92 TB Mixed-use Zainstalowane 2 dyski SAS o pojemności 2,4 TB każdy Zainstalowany dedykowany wewnętrzny napęd DVD-RW z możliwością

	wymiany na napęd Blu-ray.
Płyta główna	Dwuprocesorowa; Wyprodukowana i zaprojektowana przez producenta serwera Możliwość instalacji procesorów 26-rdzeniowych; Zainstalowany modułu TPM 2.0 8 aktywnych złącz PCI Express generacji 3 w tym: • 3 fizyczne złącza o prędkości x16; • 5 fizycznych złącz o prędkości x8; 12 gniazd pamięci RAM; Obsługa 1.5TB pamięci RAM; Wsparcie dla technologii SDDC i Advanced ECC; 2 sloty dla dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express nie zajmujące klatek dla dysków hot-plug;
Procesor	Osiągający w teście PassMark CPU Mark 20200 – załączyć wydruk ze strony https://www.cpubenchmark.net lub www.passmark.com **na wezwanie Zamawiającego**
Pamięć RAM	64 GB pamięci RAM DDR4 Registered 2933Mhz
Kontrolery LAN	Zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona w interfejsy: 2x 1Gbit Base-T Możliwość uzyskania konfiguracji posiadającej 2x1Git Base-T + 2x10Git SFP+ bez instalacji dodatkowych kart w slotach PCI Express;
Kontrolery I/O	Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug; Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache;
Porty	Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera; 2 porty USB wewnętrzne; 4 porty USB 3.0 dostępne z tyłu serwera; Opcjonalny port serial do zarządzania serwerem; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; 2 porty USB 3.0 na panelu przednim
Zasilanie, chłodzenie	Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy 800W; Redundantne wentylatory hotplug;
Zarządzanie	1. Wbudowane diody lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii

	2. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: • karty rozszerzeń zainstalowanej w dowolnym slocie PCI Express • CPU • pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM • wbudowanego na płycie głównej nośnika pamięci M.2 SSD • karty zrządzającej serwera • wentylatorów • baterii podtrzymującej ustawienia BIOS płyty głównej • zasilaczy 3. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, umożliwiający pełne zarządzanie i zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s i złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web, SSH; • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; • Zarządzanie alarmami poprzez SNMP; • Możliwość przejęcia konsoli tekstowej • Możliwość zarządzania przez kilku administratorów jednocześnie • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Obsługa serwerów proxy (autentykacja) • Obsługa VLAN • Możliwość konfiguracji parametru Max. Transmission Unit (MTU) • Wsparcie dla protokołu SSDP • Obsługa protokołów TLS 1.2, SSL v3 • Obsługa protokołu LDAP • Synchronizacja czasu poprzez protokół NTP • Możliwość backupu i odtworzenia ustawień BIOS serwera oraz ustawień karty zarządzającej 4. Oprogramowanie zarządzające i diagnostyczne producenta serwera, umożliwiające konfigurację kontrolera RAID, instalację systemów

	operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii; 5. Możliwość konfiguracji i wykonania aktualizacji BIOS, firmware, sterowników serwera bezpośrednio z GUI karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
Gwarancja	3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; Wykonawca musi posiadać ISO 9001 i 27001 na świadczenie usług serwisowych – **okazać na wezwanie Zamawiającego;** Bezpłatna dostępność poprawek i aktualizacji BIOS/firmware/sterowników dożywotnio dla oferowanego serwera;
Dokumentacja, inne	Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – oświadczenie producenta **załączyć na wezwanie zamawiającego**; Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – oświadczenie producenta **załączyć na wezwanie zamawiającego**; Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; W czasie obowiązywania gwarancji na sprzęt, po podaniu na infolinii numeru seryjnego urządzenia , możliwość weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
System operacyjny	Licencja musi uprawniać do zainstalowania w środowisku fizycznym lub dwóch instancji wirtualnych; Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

	3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Dodawanie i wymiana pamięci RAM bez przerywania pracy. 6. Dodawanie i wymiana procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu;

	18. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dwadzieścia licencji dostępowych dla użytkowników sieciowych; 23. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 24. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach; 25. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 26. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych;

	c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach; m) 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. n) Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN

	bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek; 29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 30. Mechanizmy zdalnej administracji oraz mechanizmy administracji przez skrypty. 31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

IV. Serwer Typ III z szafką zabezpieczająca i switchem – zestaw - 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Rack o wysokości maksimum 1U z możliwością instalacji 4 dysków 3,5” typu hot-swap wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	• Przystosowana do pracy ciągłej, dedykowana do pracy w serwerach; • Serwer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module v 1.2; • 3 sloty PCIe gen 3 • 1 slot PCIe gen 3 przeznaczony dla dysku z interfejsem M.2 • 6 slotów SATA3
Procesor	Osiągający w teście PassMark CPU Mark wynik 15 700 – **załączyć na wezwanie zamawiającego** wydruk ze strony https://www.cpubenchmark.net/ lub www.passmark.com
RAM	2x16GB pamięci RAM ECC UDIMM o częstotliwości pracy 2666MHz. Płyta musi obsługiwać 128GB; Na płycie głównej muszą znajdować się 4 sloty przeznaczone dla pamięci.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość 1920x1200
Wbudowane porty	4 porty USB w tym 2 porty USB 3.0 z tyłu obudowy, 1 port VGA oraz 1 port RS-232 na tylnym panelu.
Interfejsy sieciowe	Wbudowane 2 porty 1Gb Ethernet (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Wbudowany 1 port Gigabit Ethernet RJ-45 dedykowany dla karty zarządzającej
Kontroler dysków	Sprzętowy kontroler dyskowy;

	Możliwe konfiguracje poziomów RAID: 0, 1, 5, 10.
Dyski twarde	Zainstalowane 2 dyski o pojemności 1TB, 7.2RPM, Hot-Plug klasy Enterprise. Zainstalowany 1 dysk SSD SATA o pojemności 960GB, 6Gbps, Hot-Plug klasy Enterprise, 1.3 DWPD. Możliwość zainstalowania jednego dysku M.2 SATA
Napęd optyczny	Możliwość instalacji wbudowanego napędu DVD-RW
Wentylatory	4 wentylatory
Zasilacze	Zasilacz o mocy 350W o sprawności 94% przy 50% obciążeniu, i 90% sprawności przy 100% obciążeniu.
Bezpieczeństwo	• Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego • Możliwość włączania I wyłączania portów USB na obudowie • Możliwość zapisywania i odtwarzania ustawień firmware w BIOS
System operacyjny	Licencja musi uprawniać do zainstalowania w środowisku fizycznym lub dwóch instancji wirtualnych; Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Dodawanie i wymiana pamięci RAM bez przerywania pracy. 6) Dodawanie i wymiana procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w

	poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu; 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dziesięć licencji dostępowych dla urządzeń sieciowych; 23) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 24) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach;

	25) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 26) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych; c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej

	liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach; m) 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. n) Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 27) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek; 29) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 30) Mechanizmy zdalnej administracji oraz mechanizmy administracji przez skrypty. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO 27001 i ISO 28001 - **załączyć na wezwanie zamawiającego certyfikaty dla producenta**
Diagnostyka	Umieszczone na froncie obudowy lampki LED, umożliwiające wyświetlenie informacji o stanie dysków, połączenia sieciowego, zasilaniu i temperaturze.
Gwarancja	3 lata gwarancji On-Site producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia; Serwis musi być świadczony zgodnie z normą ISO 27001 – **okazać na**

	wezwanie zamawiającego certyfikat dla Wykonawcy;
Szafka rack	19" 27U stojąca, głębokość 800 mm; Nośność statyczna - 800kg Drzwi przednie przeszklone Drzwi boczne zatrzaskowe z zamknięciem na klucz i możliwością demontażu; Otwory na przewody od góry i od dołu Drzwi tylne zamykane na klucz Otwory wentylacyjne w ścianach bocznych i w drzwiach Możliwość zamontowania czterech wentylatorów w suficie Dwa komplety kluczy Gwarancja - 36 miesięcy **Panel z czterema wentylatorami:** Mocowanie: w górnej płycie szafy RACK Musi zawierać zestaw montażowy; Musi być wykonany z blachy stalowej walcowanej o grubości 1.2 mm.; Gwarancja: 24 miesiące **Listwa zasilająca 230V:** Wysokość: 1U Standard: rack 19" Liczba gniazd: 8 SCHUKO Mocowanie: czteropunktowe doczołowe Podświetlany wyłącznik Musi zawierać zestaw montażowy 4x koszyczek ze śrubą M6 i podkładką Zasilanie: 230V AC Długość przewodu: 1.8m Gwarancja: 36 miesięcy; **Patchpanel:** Liczba gniazd: 24 Wysokość: Maksymalnie 1U Standard: rack 19" Typ gniazda: keystone Mocowanie: czteropunktowe doczołowe Musi zawierać zestaw montażowy - 4x koszyczek ze śrubą M6 i podkładką; Pole opisowe nad każdym gniazdem Wykonanie: blacha stalowa walcowana o grubości 1.2 mm; Organizer kabli Gwarancja: 36 miesięcy; **Moduł keystone RJ45 kat.5e UTP – 24 szt.** **Kategoria: 5e** **Złącza: IDC110**

	Montaż beznarzędziowy **Kontakty z fosforobrązu platerowanego złotem** Kolorowe kodowanie zgodne z 568A i 568B
Switch	**Porty**: • 24 Porty RJ45 10/100/1000 Mbps • 4 Gigabitowe Sloty SFP • 1 Port konsolowy RJ45 • 1 Port konsolowy Micro-USB Bezwentylatorowy; Maksymalne zużycie energii – 20W; Wydajność przełączania – 55 Gbps; Szybkość przekierowań pakietów – 40 Mpps; Tablica adresów MAC – 8K; **QoS:** • 8 kolejek priorytetów • Priorytetowanie 802.1p CoS/DSCP • Planowanie kolejki - SP (Strict Priority) - WRR (Weighted Round Robin) - SP+WRR • Kontrola przepustowości - Ograniczenie przepustowości; • Mirror do wspieranego interfejsu - Redirect do wspieranego interfejsu; - Rate Limit - QoS Remark **Funkcje L2 i L2+:** - statyczna agregacja linków - 802.3ad LACP - Do 8 grup agregacji, zawierających 8 portów na grupę • Spanning Tree Protocol - 802.1d STP - 802.1w RSTP - 802.1s MSTP • Wykrywanie Pętli - Bazujące na Porcie i na VLAN - 802.3x Flow Control - HOL Blocking Prevention - Port Mirroring - CPU Mirroring

	- One-to-One - Many-to-One - Tx/Rx/Both **Przełączanie L3:** • 16 interfejsów IPv4/IPv6 • Statyczny routing - 48 statyczne trasy • Statyczny ARP • 316 ARP • Proxy ARP • DHCP Serwer **Zarządzanie:** • Wsparcie kontrolera sprzętowego, programowego i opartego na chmurze • Automatyczne wykrywanie urządzeń • Konfiguracja Batch • Monitorowanie sieci • Ostrzeżenia o nieprzewidzianych zdarzeniach • Harmonogram Restartów • ZTP (Zero-Touch Provisioning)*

V. Zasilacz awaryjny – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj	jednofazowy
Typ obudowy	Tower
Topologia	Line-interactive;
Rodzaj wejścia	IEC C14;
Przewód zasilający	1,5 m.
Moc VA/W	1000/550
Kształt fali przy pracy baterii	Sinus czysty lub symulowany;
AVR	Single Boost, Single buck;
Wyjście	4 x FR zabezpieczone przed przepięciami i bateriami;
Czas pracy na baterii (podtrzymania)	1 minut przy pełnym obciążeniu/ 8 min. przy połowicznym;
Czas naładowania baterii	Maksymalnie 8h;
Układ przeciwprzepięciowy	450J, ochrona sieci LAN (RJ45),
Szybkość transmisji danych Ethernet	1 Gbps;
Rozpraszanie ciepła	22 BTU/h

Hałas	Maksymalnie 40 dBA;
Czas transferu	Maksymalnie 5 ms.
Złącza	1 x USB, 1 x RJ11, 1 x RJ45, 1 x RS232
Warunki gwarancji	2 lata;
Wymagania dodatkowe	Panel LCD, bezpiecznik, uruchamianie na baterii, filtrowanie EMI/RFI

VI. Laptopy – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej
Ekran	15.6 FHD, IPS lub VA, 1920 x 1080, powłoka przeciwodblaskowa, jasność 250 nits
Wydajność	Oferowany komputer musi osiągać w teście wydajności BAPCO Sysmark 25 wynik 1250 pkt. **Wydruk z oprogramowania testującego załączyć na wezwanie Zamawiającego.** Wymagane testy wydajnościowe Wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Wykonawca dostarczy Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć RAM	16 GB z możliwością rozbudowy do 64 GB RAM, 2 sloty na pamięci w tym min. jeden wolny.
Pamięć masowa	512GB NVMe SSD Komputer musi oferować montaż dwóch dysków w konfiguracji M.2 + 2,5”
Grafika	Wynik karty graficznej w teście SysMark25 Creativity co najmniej 1300 punktów – **wynik załączyć na wezwanie Zamawiającego**.
Klawiatura	Klawiatura z wbudowanym w klawiaturze podświetleniem, (układ US). Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną; Wbudowane dwa głośniki stereo 2x2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w

	obudowę matrycy. Kamera internetowa 720p z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy. Czytnik kart microSD, 1 x port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 6 AX201 2x2 + Bluetooth 5.1
Bateria i zasilanie	40Whr. umożliwiająca szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Czas pracy na baterii - 8 godzin, potwierdzony wynikiem testu MobileMark25 Battery Life – **na wezwanie Zamawiającego** załączyć wynik testu testu lub link do publikacji na stronie BAPCO, w oferowanej konfiguracji; Zasilacz o mocy 65W;
Waga i wymiary	Maksymalnie 2 kg. z baterią
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane; Dookoła matrycy uszczelnienie chroniące klawiaturę po zamknięciu przed kurzem i wilgocią. Komputer spełniający normy MIL-STD-810H
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, Wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego odczytania co najmniej następujących informacji z BIOS: datę produkcji komputera, o kontrolerze audio, procesorze, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne pole asset tag. Możliwość ustawienia hasła dla administratora; Możliwość ustawienia hasła dla użytkownika które jednocześnie będzie blokować uruchamianie systemu z jakichkolwiek urządzeń; Możliwość konfiguracji zależności między tymi hasłem; Hasła muszą umożliwiać zawarcia w sobie znaków specjalnych, liczb i liter; Możliwość odczytania informacji o stanie naładowania baterii, stanie podpiętego zasilacza; Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania; Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
Certyfikaty	Laptop musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001 – **certyfikaty załączyć na wezwanie Zamawiającego;** Certyfikat TCO, wymagana certyfikacja na stronie: https://tcocertified.com/product-finder/ – **załączyć na wezwanie**

	Zamawiającego wydruk z strony.
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, pendrive;
Bezpieczeństwo	TPM;
Porty i złącza	Wbudowane porty i złącza: 1 x HDMI 1.4 1 x RJ-45, 2 x USB 3.1, 1 x USB 3.1 TYP-C z obsługą DP 1.2 1 x USB 2.0 port zasilania, złącze linki zabezpieczającą. Złącze do podłączenia stacji dokującej umożliwiające ładowanie laptopa.
Warunki gwarancyjne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii; Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) 3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Wykonawca musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikaty załączyć na wezwanie Zamawiającego**
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w języku polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe

	6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 9. Graficzne środowisko instalacji i konfiguracji w języku polskim 10. Wbudowany system pomocy w języku polskim. 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 16. Konta i profile użytkowników zarządzane zdalnie; 17. Praca systemu w trybie ochrony kont użytkowników. 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 19. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 20. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 26. Możliwość przywracania systemu operacyjnego do stanu początkowego

	z pozostawieniem plików użytkownika. 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 28. Wbudowany mechanizm wirtualizacji typu hypervisor; 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 40. Możliwość tworzenia wirtualnych kart inteligentnych. 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 42. Wsparcie dla IPSEC oparte na politykach; 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 44. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;

	45. Umożliwiający pracę w domenie;
Oprogramowanie użytkowe	Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - upgrade i instalację wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość sprawdzenia przed instalacją każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta, a w szczególności informacji : a) poprawkach i usprawnieniach dotyczących aktualizacji b) dacie wydania ostatniej aktualizacji c) priorytecie aktualizacji d) zgodności z systemami operacyjnymi e) jakiego komponentu sprzętu dotyczy aktualizacja f) wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika lub aplikacji; - rozpoznawanie modelu oferowanego komputera, w tym numeru seryjnego komputera; - sprawdzenie historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą i wersją - wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością export; - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych, ściągniętych, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów dotyczyły, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu; Raport musi zawierać dokładną datę i godzinę z podjętych i wykonanych akcji/zadań;

VII. Oprogramowanie antywirusowe 22 szt. (2 jednostki organizacyjne zarządzane w osobnych panelach administracyjnych – 8 i 14 licencji)

System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej:

1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,

2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
3. Stosowanie kwarantanny
4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
5. Skanowanie urządzeń USB natychmiast po podłączeniu,
6. Automatyczne odłączanie zainfekowanej końcówki od sieci,
7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach.
9. Musi posiadać moduł ochrony IDS/IPS
10. Musi posiadać mechanizm wykrywania skanowania portów
11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości
13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH.
14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej.
15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom.
16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji;
17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji.
18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji.
20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji.
21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.

22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware.
23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware;
24. Centralna konsola zarządzająca umożliwiająca co najmniej:
    a) przechowywanie danych w bazie typu SQ
    b) zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory;
    c) tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux
    d) centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerze konsoli;
    e) raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich;
    f) definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji;
25. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera;
26. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach;
27. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
28. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.
29. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;
30. System musi umożliwiać, z konsoli na serwerze, co najmniej:
    a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
    b) przyznawanie praw dostępu dla nośników pamięci tj. USB, CD
    c) regulowania połączeń WiFi i Bluetooth
    d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
    e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi
    f) blokowanie dostępu dowolnemu urządzeniu
    g) tymczasowe dodanie dostępu do urządzenia przez administratora
    h) szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych;
    i) zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
    j) zezwalać na dostęp tylko urządzeniom wcześniej dodanym przez administratora

k) używania tylko zaufanych urządzeń sieciowych;

31. Funkcja wirtualnej klawiatury
32. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie
33. Możliwość dodania własnych aplikacji do listy zablokowanych
34. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze
35. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
36. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki;
37. Możliwość zablokowania funkcji Printscreen
38. Monitorowanie przesyłu danych między aplikacjami;
39. Monitorowanie i kontrola przepływu poufnych informacji
40. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj
41. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe;
42. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe
43. Ochrona zawartości schowka systemu
44. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
45. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych
46. Ochrona plików zamkniętych w archiwach
47. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
48. Możliwość tworzenia profilu DLP dla każdej polityki
49. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
50. Ochrona przez wyciekiem plików poprzez programy typu p2p
51. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
52. Monitorowanie określonych rodzajów plików.
53. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania.
54. Możliwość śledzenia zmian we wszystkich plikach
55. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych;
56. Możliwość definiowana własnych typów plików
57. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
58. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
59. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich
60. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;.
61. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
62. Musi posiadać możliwość eksportu danych użytkownika
63. Import listy urządzeń z pliku CSV

64. Dodawanie urządzeń;
65. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta
66. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,;
67. Podgląd zainstalowanych aplikacji;
68. Moduł raportowania aktywności, skanowania oraz naruszenia reguł;
69. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową;
70. Portal zarządzający w postaci SaaS;
71. Skanowanie podatności za pomocą nodów skanujących;
72. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
73. Portal zarządzający musi umożliwiać:
    a) przegląd wybranych danych;
    b) zablokowanie możliwości zmiany konfiguracji;
    c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów;
    d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
    e) eksport skanów podatności do pliku CSV;
74. Licencja bezterminowa z 3 letnim prawem do aktualizacji samej aplikacji oraz bazy sygnatur
75. **D**eduplikacja danych na źródle,
76. Backup przyrostowy i różnicowy,
77. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
78. Backup danych lokalnych – plikowy oraz poczty;
79. Backup otwartych plików;
80. Filtr plików oraz folderów,
81. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),
82. Przywracanie danych do wskazanej lokalizacji,
83. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
84. Wyszukiwanie plików w repozytorium użytkownika,
85. Automatyczne logowanie,
86. Zapamiętywanie danych logowania,
87. Automatyczne uruchamianie programu przy starcie systemu,
88. Ustawianie priorytetu dla procesu backupu,
89. Zmiana klucza szyfrującego,
90. Konfiguracja wydajności procesu backupu,
91. Zastępowanie nazwy pliku GUID-em,

92. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,
93. Kompresja danych,
94. Transmisja po bezpiecznym protokole TLS,
95. Deklaracja klucza szyfrującego dane użytkownika,
96. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
97. Obliczanie sumy kontrolnej,
98. Kopie zapasowe muszą być przechowywane w data center, na terenie Polski.
99. Licencje muszą być przypisywane do urządzenia z limitem pojemności przestrzeni w chmurze minimum 50 GB;
100. Wsparcie techniczne, świadczone w języku polskim;

VIII. Access Point – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Standardy	Wi-Fi 6 IEEE 802.11ax/ac/n/a 5 GHz IEEE 802.11ax/n/b/g 2,4 GHz
Zasięg sieci WiFi	6 zintegrowanych anten Beamforming 4T4R
Wydajność sieci WiFi	Dwa pasma MU-MIMO 4×4 OFDMA Ograniczanie nieefektywnego wykorzystywania przepustowości pasm DFS 6 strumieni
Tryby pracy	Tryb routera Tryb punktu dostępowego;
Procesor	Trzyrdzeniowy z taktowaniem 1,5 GHz
Porty Ethernet	1 gigabitowy port WAN 4 gigabitowe porty LAN Statyczna agregacja łączy dostępna na dwóch portach LAN
Obsługiwane typy USB	1 port USB 3.0 Obsługiwane typy partycji: NTFS, exFAT, HFS+, FAT32 Obsługiwane funkcje: Serwer FTP Serwer mediów Serwer Samba
Szyfrowanie sieci WiFi	WPA, WPA2, WPA3

	WPA/WPA2-Enterprise (802.1x)
Ochrona sieci	Zapora sieciowa SPI Kontrola dostępu Wiązanie adresów IP i MAC ALG Ochrona urządzeń w czasie rzeczywistym Blokowanie złośliwych witryn System zapobiegania włamaniom Zapobieganie atakom DDoS Skanowanie sieci
Sieć dla gości	5 GHz i 2,4 GHz
Serwer VPN	OpenVPN, PPTP
Wspierane protokoły	IPv4, IPv6
Kontrola rodzicielska	Profile użytkowników Biblioteka filtrowania treści Blokada dostępu Statystyki spędzania czasu online Zawieszanie dostępu do Internetu Raporty tygodniowe i miesięczne
Typy sieci WAN	Dynamiczne i statyczne przydzielanie adresów IP PPPoE PPTP L2TP
QoS	dla urządzeń
Cloud	Automatyczne aktualizacje firmware'u DDNS
Przekierowywanie NAT	Port Forwarding Port Triggering DMZ UPnP
IPTV	IGMP Proxy IGMP Snooping Bridge VLAN tagowany
DHCP	Rezerwacja adresów Lista klientów DHCP Serwer DHCP
DDNS	NO-IP DynDNS

Zarządzanie	Aplikacja dedykowana Przeglądarka
Gwarancja	3 lata;

IX. Urządzenie wielofunkcyjne – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ urządzenia	Kolor
Funkcje	Drukowanie, Kopiowanie i skanowanie;
Rozmiar papieru	A3
Pamięć	128 MB
Rozdzielczość druku	4800 x 1200 dpi;
Szybkość wydruku (mono/kolor)	35/25 str./min.
Obsługiwane formaty	A3, A4, A5, A6, Com-10, C5;
Obsługa papieru	Podajnik na 250 arkuszy i ADF na 50 arkuszy Odbiornik na 100 arkuszy A4/50 arkuszy A3
Komunikacja	Przewodowa i 802.11 b/g/n, USB, wifi direct;
Rozdzielczość kopiowania	1.200 x 4.800 dpi
Szybkość kopiowania (kolor/mono)	9/12 obrazów na minutę
Rozdzielczość skanowania	1,200 x 2,400 dpi
Szybkość skanowania	14 obrazów na minutę;
Skanowanie do	Email, plik, pamięć USB, serwer, FTP, udział sieciowy;
Zużycie energii podczas pracy	Maksymalnie 30W
Poziom hałasu podczas pracy	Maksymalnie 50 dB
Materiały eksploatacyjne	500 stron w zestawie z urządzeniem; Możliwość zastosowania wkładów czarnych na 3000 stron i kolorowych na 1500 stron;
Gwarancja	3 lata;
Wymagania dodatkowe	Wyświetlacz 6 cali, automatyczny dupleks;

X. Serwer NAS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Osiągający w teście PassMark Average CPU Mark wynik 5200 pkt- **załączyć na wezwanie Zamawiającego wydruk ze strony www.cpubenchmark.net**
Pamięć	32 GB z możliwością rozbudowy do 64 GB ;
Pamięć flash	5 GB z ochroną systemu operacyjnego przed podwójnym rozruchem

Zatoki na dyski	5 x 3,5 cala i 4 x 2,5 cala;
Obsługiwane dyski	2,5 cala SATA , SSD SATA, SSD U.2 NVMe PCIe Gen3 x4 oraz 3,5 cala SATA; hot swap;
Porty	2 x 2,5 GbE, 1 x 10 GbE Base-T, 4 x USB 3.2, w tym 1 x USB-C;
Obudowa	Rack lub tower
Diody	LAN, USB, zatoki dyskowe;
Zasilacz	Maksymalnie 120W;
Wentylator	1 x 10 mm;
Połączenia CIFS	2000;
Rozmiar puli	300 TB;
Ilość pul	128
Zainstalowane dyski	4 x 4 TB SATA 6 Gb/s; Pamięć podręczna cache – 256 MB; Prędkość obrotowa – 7200 rpm;
Pobór mocy podczas pracy	Maksymalnie 60W;
System operacyjny	1. Pula pamięci SED; 2. Obsługiwany rozmiar woluminu – 250 TB; 3. Liczba folderów udostępnianych – 512; 4. Rozmiar folderu udostępnianego – 250 TB; 5. Rozszerzenie JBOD; 6. VJBOD; 7. Usługa iSCSI i FC; 8. Jednostka iSCSI LUN oparta na plikach i blokach; 9. Funkcje LUN: 10. Mapowanie LUN; 11. Przenoszenie jednostki LUN między iSCSI i FC; 12. Maskowanie LUN 13. Import/eksport aliasów WWPN 14. Wiązanie portu FC 15. Wielościeżkowe we/wy (MPIO) 16. Rozszerzenie pojemności jednostek LUN online 17. Migawka jednostki LUN 18. Replikacja migawek jednostek LUN i klonowanie; 19. Automatyczne warstwowanie; 20. Obsługa RAID - JBOD, RAID 0, 1; 21. Migracja RAID; 22. Rozszerzenie RAID i puli pamięci; 23. Hot spare RAID; 24. Szacowanie żywotności dysków SSD;

	25. Migawka jednostki LUN; 26. 64 migawki na urządzenie i 32 na jednostkę LUN; 27. Interwał migawki – 5 minut; 28. Samoobsługowe odzyskiwanie migawek; 29. Migawka złożona z aplikacji; 30. Pamięć podręczna do odczytu i zapisu; 31. Narzędzie do profilowania SSD; 32. Zarządzanie zewnętrznym urządzeniem RAID; 33. Serwer plików; 34. Serwer FTP; 35. Kontroler domeny; 36. Limitowanie liczby użytkowników; 37. Monitor zasobów; 38. SNMP v2 i 3 39. Odzyskiwanie plików usuniętych ; 40. Automatyczne czyszczenie i filtr typu pliku 41. Dziennik systemowy i centrum powiadomień; 42. Harmonogram włączania i wyłączania; 43. Przełącznik wirtualny; 44. Trunkowanie portów; 45. Serwer DHCP;
Gwarancja	2 lata;
Wymagania dodatkowe	Przyspieszanie pamięci SSD, WoL, szyny do montażu w szafie w przypadku obudowy rack, złącze Kensingotn,

XI. Przełącznik – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Liczba portów	12 szt., w tym 4 x 10GbE SFP+ i 8 x combo 10GbE SFP+/RJ45; Porty 10GbE SFP+ muszą być wstecznie kompatybilne z 1GbE SFP; Port combo RJ45 (miedziany) musi obsługiwać następujące prędkości: 10 Gb, 5Gb, 2,5Gb, 1Gb, 100Mb;
Zużycie energii podczas pracy	Maksymalnie 50W;
Tabela z adresami MAC	32K
Łączna przepustowość	120 Gb/s
Zdolność przełączania	240 Gb/s
Ramki Jumbo	9k
Wymagania dodatkowe	zgodność z normami IEEE 802.3ab, IEEE 802.3bz, IEEE 802.3an,

	IEEE 802.3ae, IEEE 802.3x, IEEE 802.3az,
Gwarancja	2 lata;

XII. Oprogramowanie biurowe – 11 szt.

Kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wymagania odnośnie interfejsu użytkownika:
   a) Pełna polska wersja językowa interfejsu użytkownika;
   b) Prostota i intuicyjność obsługi, pozwalająca na prace osobom nieposiadającym umiejętności technicznych;
   c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:
   a) posiada kompletny i publicznie dostępny opis formatu,
   b) ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   c) umożliwia wykorzystanie schematów XML
   d) wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
4. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
   d) Narzędzie do zarządzania informacja prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
7. Edytor tekstu musi umożliwiać:

a) Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
b) Wstawianie oraz formatowanie tabel
c) Wstawianie oraz formatowanie obiektów graficznych
d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
f) Automatyczne tworzenie spisów treści
g) Formatowanie nagłówków i stopek stron
h) Sprawdzanie pisowni w języku polskim
i) Śledzenie zmian wprowadzonych przez użytkowników
j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
k) Określenie układu strony (pionowa/pozioma)
l) Wydruk dokumentów
m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
n) Prace na posiadanych przez Zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
r) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

8. Arkusz kalkulacyjny musi umożliwiać:
a) Tworzenie raportów tabelarycznych
b) Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych
c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
e) Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
g) Wyszukiwanie i zamianę danych
h) Wykonywanie analiz danych przy użyciu formatowania warunkowego
i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
j) Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
k) Formatowanie czasu, daty i wartości finansowych z polskim formatem
l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m) Zachowanie pełnej zgodności z formatami posiadanych przez Zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
a) Prezentowanie przy użyciu projektora multimedialnego
b) Drukowanie w formacie umożliwiającym robienie notatek
c) Zapisanie w postaci tylko do odczytu.
d) Nagrywanie narracji dołączanej do prezentacji
e) Opatrywanie slajdów notatkami dla prezentera
f) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
g) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
h) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
i) Tworzenie animacji obiektów i całych slajdów
j) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
k) Pełna zgodność z formatami plików posiadanych przez Zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.

10. Narzędzie do zarządzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców

c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
d) Automatyczne grupowanie poczty o tym samym tytule
e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g) Zarządzanie kalendarzem
h) Udostępnianie kalendarza innym użytkownikom
i) Przeglądanie kalendarza innych użytkowników
j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
k) Zarządzanie lista zadań
l) Zlecanie zadań innym użytkownikom
m) Zarządzanie listą kontaktów
n) Udostępnianie listy kontaktów innym użytkownikom
o) Przeglądanie listy kontaktów innych użytkowników
a) Możliwość przesyłania kontaktów innym użytkowników

11. Licencja niewygasająca do użytku komercyjnego. Nie dopuszcza się licencji w modelu subskrypcyjnym;

XIII. Zestaw sieciowy – 1 szt.

1. Przełącznik – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Standardy	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.1q, IEEE 802.1p
Porty	24 porty RJ45 10/100/1000 Mb/s Autonegocjacja/AUTO-MDI/MDIX
Okablowanie	Współpraca z okablowaniem kategorii 6
Obudowa	Rack;
Zużycie energii podczas pracy	Maksymalnie 15W;
Ilość generowanego ciepła	Maksymalnie 50 BTU/h
Wydajność przełączania	48 Gb/s
Szybkość przekierowań pakietów	35 Mp/s
Tablica adresów MAC	8K
Bufor pakietów	4 Mbit
QoS	Priorytetowanie w oparciu o port/802.1p/DSCP 4 kolejki priorytetowania Możliwość ograniczania prędkości transmisji dla każdego z portów Storm Control
Cechy przełącznika warstwy 2	IGMP Snooping Statyczna agregacja połączeń Mirroring portów Diagnostyka stanu kabli Zapobieganie pętlom
Sieci VLAN	Jednoczesna obsługa 32 VLAN z 4000 identyfikatorów VLAN; MTU Port, Tag VLAN
Metoda transmisji	Store-And-Forward
Wymagania dodatkowe	Bezwentylatorowy,
Gwarancja	3 lata;

2. Szafka rack – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj szafy	Wisząca, dwusekcyjna (dzielona); Wpusty kablowe na dole i górze szafki;
Wysokość użytkowa	9U
Szerokość użytkowa	19"

Wysokość zewnętrzna	500 mm
Szerokość zewnętrzna	600 mm
Głębokość	550 mm
Drzwi frontowe	Pełne, metalowe, zamykane na zamek; Możliwość otwierania drzwi na prawo lub lewo zależnie od sposobu montażu;
Tył szafy	Otwarty
Listwy montażowe	Szyny rack do montażu urządzeń
Wentylacja aktywna	Miejsce na wentylator wraz z otworami montażowymi na górze i na dole szafy.
Wentylacja pasywna	Otwory wentylacyjne na górze i na dole szafy
Wymagania dodatkowe:	Złącza uziemiające w drzwiach i podstawie szafy 2 pary kluczy; Półka' Wentylator;
Gwarancja	3 lata;

3. Łącznik modularny – 30 szt.

1. RJ45 kat. 5e, UTP (keystone)
2. Musi być przeznaczony do:
   a) połączenia dwóch przewodów typu skrętka komputerowa zakończonych złączem RJ45
   b) połączenia 4-parowych przewodów nieekranowanych (UTP) kategorii 5e.
   c) połączenia patchcordami RJ45-RJ45
3. Rodzaj złącza: pojedyncze RJ45;
4. Łącznik przewodów zakończonych RJ45-R45;
5. Adapter umożliwiający montaż złącza w modułach Keystone;
6. Mocowanie: mechanizm zatrzaskowy;
7. Gwarancja – 3 lata;

4. UPS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj	jednofazowy
Typ obudowy	Tower
Topologia	Line-interactive;
Rodzaj wejścia	IEC C14;
Przewód zasilający	1,5 m.
Moc VA/W	1000/550
Kształt fali przy pracy	Sinus czysty lub symulowany;

baterii	
AVR	Single Boost, Single buck;
Wyjście	4 x FR zabezpieczone przed przepięciami i bateriami;
Czas pracy na baterii (podtrzymania)	1 minut przy pełnym obciążeniu/ 8 min. przy połowicznym;
Czas naładowania baterii	Maksymalnie 8h;
Układ przeciwprzepięciowy	450J, ochrona sieci LAN (RJ45),
Szybkość transmisji danych Ethernet	1 Gbps;
Rozpraszanie ciepła	22 BTU/h
Hałas	Maksymalnie 40 dBA;
Czas transferu	Maksymalnie 5 ms.
Złącza	1 x USB, 1 x RJ11, 1 x RJ45, 1 x RS232
Warunki gwarancji	2 lata;
Wymagania dodatkowe	Panel LCD, bezpiecznik, uruchamianie na baterii, filtrowanie EMI/RFI

Zamawiający zastrzega sobie możliwość wezwania Wykonawcy, którego oferta została najwyżej oceniona, do okazania zaoferowanego sprzętu i oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SWZ.
Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe).
Niestawienie się Wykonawcy w wyznaczonym czasie i miejscu na okazaniu (prezentacji) sprzętu i/lub oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez Wykonawcę wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.

Część II - Oprogramowanie do monitoringu komputerów

	Specyfikacja Techniczna Oprogramowania
1.	Oprogramowanie winno posiadać budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów dla 20 jednostek komputerowych.
2.	Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana ma być co najmniej przy użyciu szyfrowanego protokołu TLS 1.2.
3.	Moduły mają umożliwiać kompleksową 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.	Program winien mieć możliwość wykorzystywania darmowego silnika bazy danych z kodem źródłowym dostępnym na licencji open-source (np. PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych.
5.	Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., mają być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Mają być również grupowane w osobnym, dedykowanym oknie. Pozwali to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
6.	Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty ma być kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów.
7.	Program ma posiadać 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.
8.	Działania administratorów mają być automatycznie eksportowane do zewnętrznego kolektora Syslog.
	MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) **ma zawierać:**

9.	Monitorowanie obejmować ma serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle
10.	Wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
11.	Wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
12.	Wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
13.	Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
14.	Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
15.	Wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.
16.	Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
17.	Wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
18.	Zablokowania mapy urządzeń przed przypadkową edycją.
19.	Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program ma monitorować czas ich odpowiedzi i procent utraconych pakietów.
20.	Serwery pocztowych monitorowane w zakresie: - czas logowania do serwisu odbierającego oraz czas wysyłania poczty, -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), - wykonywania operacji testowych, - wysłania powiadomienia jeśli serwer pocztowy nie działa.
21.	Monitorowanie serwerów WWW i adresów URL.
22.	Cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.
23.	Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
24.	Obsługi 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.

25.	Obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
26.	Monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych – graficzna prezentacja panelu switcha, - ruchu generowanego przez podłączone do portów stacje robocze.
27.	Serwisy Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.
28.	Wyświetlania 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.
29.	Wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
30.	Program ma posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program ma posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
31.	Nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów 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. Alarmy budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.
32.	Integracjia programu ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).
	W ZAKRESIE INWENTARYZACJI
33.	Program ma automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp., zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
34.	Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio

	umożliwi audytowanie i weryfikację użytkowania licencji w organizacji.
35.	Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
36.	Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
37.	Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
38.	Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
39.	Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
40.	Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy) 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).
41.	Umożliwia wymianę plików do i ze stacją roboczej poprzez funkcję Menedżera plików.
42.	Działania administratorów wykonywane w tej funkcji są logowane.
43.	Moduł inwentaryzacji zasobów ma umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: ✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, ✓ tworzenia powiązań między zasobami a urządzeniami, ✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, ✓ wskazania osób uprawnionych do użycia zasobów, ✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, ✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, ✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, ✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, ✓ importu danych z zewnętrznego źródła (.CSV), przechowywania dowolnych dokumentów

	(np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., ✓ tworzenia powiązań między zasobami a dokumentami w relacji 1:N, ✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., ✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, ✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, ✓ przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, ✓ konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, ✓ konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, ✓ archiwizacji i porównywania audytów zasobów, ✓ tworzenia kodów kreskowych dla zasobów, ✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, ✓ inwentaryzacji 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, ✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), ✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).
44.	Dodatkowo ma być dostępny Agent inwentaryzacji na system Android.
45.	Inwentaryzacja oprogramowania ma zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: 1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji. 4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji. 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

	10. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. 11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. 12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp.
46.	Inwentaryzacja oprogramowania ma zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: 1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji. 4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji. 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. 11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. 12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp.
47.	Okna audytowe mają posiadać możliwość filtrowania elementów per oddział.
	W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW
48.	Program ma umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie: ✓ Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), ✓ Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, ✓ Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja

	była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, ✓ Informacji o edytowanych przez użytkownika dokumentach, ✓ Historii pracy (cykliczne zrzuty ekranowe), ✓ Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), ✓ Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), ✓ Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty 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.
49.	Program ma mieć możliwość monitorowania kosztów wydruków, nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
50.	Program ma mieć możliwości: ✓ blokowania 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. ✓ blokowania ruchu na wskazanych portach TCP/IP, ✓ blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, ✓ wysyłania 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, ✓ przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), ✓ definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
51.	Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
52.	Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
53.	Program ma posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron

	internetowych.
	REALIZACJA ZDALNEJ POMOCY UŻYTKOWNIKOM
54.	W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. Niniejszym moduł obejmuje bazę zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
55.	Program ma umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.
56.	Umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.
57.	W skład modułu ma wchodzić również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic).
58.	Program ma dawać możliwość informowania pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Dostęp do systemu zgłoszeń oraz bazy wiedzy ma być wykonywany przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.
59.	Funkcjonalność modułu ma umożliwiać uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.
60.	Moduł pomocy zdalnej ma ma siadać funkcjonalności: ✓ pobieranie listy użytkowników z Active Directory,

	✓ zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, ✓ zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, ✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej, ✓ tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, ✓ automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, ✓ procesowanie zgłoszeń użytkowników z wiadomości e-mail, ✓ tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, ✓ wykonywanie operacji na wielu zgłoszeniach równocześnie, ✓ dołączanie załączników do zgłoszeń, ✓ rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, ✓ szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, ✓ wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, ✓ zrzuty ekranowe (podgląd pulpitu), ✓ dystrybucję oprogramowania przez Agenty, ✓ dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), ✓ zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, ✓ możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, ✓ planowanie nieobecności pracowników helpdesk, ✓ obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, ✓ generowanie raportów obsługi helpdesk, ✓ zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), ✓ zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), ✓ wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.
	MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM zapewniająca:
61.	Blokowanie urządzeń i nośników danych. Program zarządza 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.
62.	Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
63.	Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
64.	Blokownie ma dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
65.	Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
66.	Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
67.	Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
68.	Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
69.	Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.
	Zarządzanie prawami dostępu do urządzeń
70.	Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
71.	Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane
72.	Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
73.	Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
74.	Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
	Audyt operacji na plikach na urządzeniach przenośnych
75.	Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
76.	Podłączenie/odłączenie urządzenia przenośnego.
	Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika
77.	Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.
	WSPIERA ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI

	UŻYTKOWNIKÓW
78.	Dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji ma mieć możliwość oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Ma mieć możliwość uzyskania dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mają mieć możliwość uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik ma mieć możliwość przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły mają umożliwić zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany ma być przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.
79.	Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
80.	Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
81.	Statystyki aktywności podwładnych widoczne dla przełożonego.
82.	Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
83.	Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
84.	Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
85.	Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
86.	Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
87.	Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
88.	Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
89.	Wskaźnik czasu poświęconego na aktywność produktywną.
90.	Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.

91.	Możliwość przypisywania kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
92.	Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.
	Portal informacyjny w formie platformy WWW
93.	Oprogramowanie ma posiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety winny być rozłożone na siatce o rozmiarze ustalonym przez administratora.
94.	Zawartość każdego z paneli informacyjnych ma być automatycznie odświeżana oraz ma być: ✓ Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem. ✓ Wyświetlana w trybie jasnym lub nocnym.
95.	Oprogramowanie ma umożliwiać zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.
96.	Widgety mają prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania: ✓ Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci, ✓ Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów, ✓ Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, ✓ Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie, ✓ Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), ✓ Produktywność dla grupy, Statystyki czasu nieproduktywnego.
97.	Program ma być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
98.	Ma istnieć możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
99.	Program dostępny ma być w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

Część III - Zakup specjalizowanego oprogramowania - Rozwiązanie do zarządzania logami, SEM/ SIEM o wydajności do 2,000 zdarzeń/ sekunda i minimalnej wielkości baz danych 12TB)

Ogólne wymagania systemowe

1	System musi zostać dostarczony w formie rozwiązania sprzętowego wyposażonego w zintegrowany interfejs web dla administratorów i operatorów systemu. System nie może wymagać instalowania innych systemów ani aplikacji realizujących dodatkowe funkcjonalności (poza zbieraniem logów z lokalizacji zdalnych oraz z systemów Windows). Wymagane jest dostarczenie broszury szczegółowo przedstawiającej parametry systemu.
2	System musi umożliwiać rozbudowywanie natywnie dostępnych funkcjonalności (min. klasyfikacja, parsowanie, alterowanie oraz filtrowanie) poprzez tzw. programowanie wizualne, które polega na tworzeniu kodu z graficznych bloków reprezentujących określone instrukcje i funkcje. Programowanie wizualne musi umożliwiać tworzenie kodu przez osoby posiadające podstawową wiedzę programistyczną (wymagana znajomość min. instrukcji warunkowych, pętli, zmiennych) a system musi posiadać możliwość testowania i weryfikowania poprawności logiki tworzonego kodu.
3	System musi być wyposażony w pojedynczy, zunifikowany interfejs graficzny web dostępny z poziomu wybranej przeglądarki (przykładowo: Google Chrome, Mozilla Firefox, Opera) umożliwiający dostęp do logów, tworzenia alertów i parserów, raportów oraz zarządzania systemem. Wszystkie operacje konfiguracji, zarządzania i analizy logów muszą być wykonywane przez ten interfejs. Wiele różnych interfejsów nie jest dopuszczalne.
4	Interfejs graficzny systemu musi umożliwiać łatwe klasyfikowanie danych wejściowych (logów) na potrzeby dalszego procesowania. Klasyfikowanie powinno umożliwiać przypisywanie określonych logów do odpowiednich parserów oraz nadawanie im tagów, ułatwiających dalszą pracę z logami (np. wyszukiwanie). Logika klasyfikacji powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. Wymagane jest dostarczenie referencji do dokumentacji opisującej tą funkcjonalność.
5	System musi umożliwiać filtrowanie nieistotnych zdarzeń na etapie klasyfikacji. Logika filtrowania powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. Wymagane jest dostarczenie dokumentacji opisującej ten proces.
6	System nie może umożliwiać modyfikacji bądź manualnego usunięcia logów zapisanych w bazie. Każdy log musi posiadać unikalny identyfikator, który umożliwi jego jednoznaczne rozróżnienie.
7	System musi umożliwiać proste wyszukiwanie zapisanych w bazie logów i tworzenie raportów w formie graficznej bez konieczności wykorzystania dedykowanego języka programowania lub zapytań SQL. Wyszukiwanie i raporty muszą być integralną częścią oferowanego systemu i być dostępne przez interfejs graficzny web. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia raportów.

8	System musi umożliwiać prezentowanie logów w formie wykresów, zgrupowanych w tzw. widokach (dashboard). Widoki muszą być dynamicznie aktualizowane i interaktywne (tzw. "drill down" - przykładowo: wybranie wartości przedstawionej na jednym wykresie powoduje automatyczne utworzenie filtru wyszukiwania w oparciu o wybraną wartość i dostosowanie pozostałych wykresów).
9	System musi udostępniać pre-definiowane widoki danych (dashboards) podzielone na kategorie pod względem typu lub producenta urządzenia źródłowego lub aplikacji.
10	System musi automatycznie aktualizować zapisane widoki z każdą nową wersją oprogramowania.
11	Dane przechowywane w okresie oczekiwanej retencji muszą być dostępne do przeszukiwana natychmiastowo, bez wprowadzania opóźnienia w postaci importu z zewnętrznych baz danych lub ich dekompresji.
12	W przypadku przeciążenia systemu, logi nie mogą być tracone. Wszystkie nie obsłużone logi muszą być buforowane, a administrator systemu powiadamiany w momencie w którym bufor zacznie się zapełniać. Bufor nie może być mniejszy nić 50GB.
13	Wykonawca musi dostarczyć potwierdzenie w formie certyfikatu, że system spełniania wymogi ISO/IEC 27001:2013 w zakresie rekordów audytowych.
14	System musi posiadać kompletną dokumentację. Dokumentacja odnosząca się do zewnętrznych źródeł nie jest dopuszczalna. Wymagane jest dostarczenie dokumentacji w formie elektronicznej lub link do wersji online w celu weryfikacji.
15	Przestrzeń dyskowa dostępna do przechowywania logów w oferowanym systemie musi wynosić przynajmniej 12TB.
16	Wymagana jest możliwość usunięcia jednego fizycznego dysku z systemu bez utraty danych lub wpływu na działanie systemu. Redundancja dysków nie może wpływać na wymaganą przestrzeń dyskową.
17	System musi informować o przekroczeniu krytycznych wartości wykorzystania dostępnych zasobów sprzętowych.
18	System musi umożliwiać wykorzystanie REST-API do integracji z zewnętrznymi systemami do monitoringu (np.: Zabbix, Nagios, MRTG etc.). Wymagane jest przedstawienie kompletnej instrukcji integracji z wybranym systemem monitoringu.
19	System musi umożliwiać łatwe tworzenie ról definiujących poziom dostępu użytkowników do zapisanych logów oraz poszczególnych elementów systemu. Wymagane jest dostarczenie dokumentacji opisującej sposób tworzenia ról użytkowników.
20	System musi umożliwiać integrację z systemem LDAP w celu logowania użytkowników. W przypadku awarii systemu LDAP, system musi umożliwiać logowanie lokalne.
21	System musi umożliwiać skalowanie pod kątem wydajności.
	Źródła
22	System musi być w stanie odbierać i procesować logi, zdarzenia i inne dane maszynowe wykorzystując co najmniej następujące protokoły: UDP/TCP SYSLOG, TCP RELP (nieszyfrowany), TCP RELP (szyfrowany). Wymagane jest dostarczenie schematu przepływu

danych oferowanego systemu.

23 System musi umożliwiać integrację z bazami danych przynajmniej MSSQL, MySQL, Oracle i PostgreSQL poprzez konektor ODB (integracja rozumiana jako możliwości pobierania całych wierszy wybranych tabel w bazie). Wymagane jest dostarczenie dokumentacji opisującej proces konfiguracji konektora ODBC.

24 System musi umożliwiać integrację z platformą wirtualizacji Vmware (ESXi, vSphere) poprzez dedykowany konektor pobierający logi I zdarzenia bezpośrednio z platformy. Wymagane jest dostarczenie dokumentacji opisującej proces konfiguracji konektora.

25 System musi umożliwiać zbieranie logów i zdarzeń z systemów Windows poprzez dedykowanego agenta instalowanego na stacji końcowej/serwerze. Agent musi być centralnie zarządzany z konsoli systemu.

26 System musi umożliwiać odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł.

27 System musi umożliwiać zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.

28 System musi umożliwiać procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe.

29 System musi umożliwiać zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów. Proszę dostarczyć dokumentację opisującą proces konfiguracji connectora Office365.

30 System musi umożliwiać monitorowanie źródeł logów i tworzenie reguł mających na celu powiadamianie administratora systemu w przypadku w którym źródło logów zdefiniowane w regule nie wyśle logów w określonym interwale.

31 System musi być dostarczony wraz z parserami do obsługi logów generowanych przez urządzenia najpopularniejszych dostawców rozwiązań IT oraz umożliwiać tworzenie własnej logiki parsowania dla nietypowych źródeł.

Parsowanie

32 System musi umożliwiać tworzenie własnych parserów logów przy wykorzystaniu programowania wizualnego z poziomu interfejsu graficznego web. Wymagane jest dostarczenie dokumentacji zawierającej czytelną instrukcję tworzenia parserów.

33 System musi umożliwiać weryfikację poprawności działania własnych parserów w trakcie ich pisania. Podczas tworzenia lub modyfikacji parsera musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez zastosowanie jej do przykładowego logu i wyświetlenie ostatecznej wersji w jakiej log zostanie zapisany w bazie jeżeli testowany parser zostanie użyty. W przypadku wystąpienia błędów w logice parsera, system powinien poinformować o tym użytkownika. Wymagane jest dostarczenie dokumentacji opisującej ten proces.

34 System w procesie parsowania musi normalizować odbierane logi do ujednoliconego formatu poprzez przypisanie poszczególnych wartości logu do odpowiadających im kluczy (format klucz = wartość). Każdy z utworzonych w procesie parsowania kluczy powinien być

oddzielnie indeksowany w bazie danych aby umożliwić szybkie wyszukiwanie wartości skojarzonych z danym kluczem.

35 System musi domyślnie zapisywać oryginalną wersję odbieranych logów.

36 Zintegrowane w systemie parsery powinny automatycznie wzbogacać procesowane logi o odpowiednią kategorię. Wymagane jest rozróżnianie przynajmniej następujących typów logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji. Musi istnieć możliwość dodania ww. kategorii podczas tworzenia własnych parserów.

37 System w procesie parsowania musi umożliwiać zamianę wybranych wartości logu na podstawowe typy (integer, float), w celu wykonywania na nich operacji matematycznych (suma, średnia, największa/najmniejsza wartość etc.) podczas prezentowania ich na dashboardach.

38 Parsery muszą umożliwiać wykorzystanie operacji matematycznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz operacji natywnego kodowania/dekodowania URL. Te operacje muszą umożliwiać tworzenie logiki mającej na celu tworzenie linków URL do zewnętrznych systemów oraz połączenie narzędzia z zewnętrznymi aplikacjami.

39 W procesie parsowania system musi dodawać własny znacznik czasu do odbieranych logów i wykorzystywać go podczas przeglądania danych. Jednocześnie system musi zachowywać oryginalny znacznik czasu z odebranych logów.

40 Tworzenie własnych parserów musi umożliwiać ustawienie typu wartości jako adres MAC i identyfikację producenta urządzenia sieciowego.

41 System w procesie parsowania musi automatycznie wzbogacać wartości IP wyekstraktowane z pól logu o powiązany rekord DNS i dane GeoIP aby umożliwić ich graficzną reprezentację na widoku mapy świata bez konieczności wykorzystania zewnętrznych usług bądź aplikacji.

42 System powinien umożliwić odbieranie wszystkich rodzajów logów. W przypadku nie istnienia odpowiedniego parsera dla odbieranego logu, system powinien zapisać go w bazie danych w formie RAW i umożliwić jego wyszukiwanie.

43 System musi automatycznie wzbogacać logi o tzw. metadane czyli informacje opisujące dany log (przykładowo: typ źródła, protokół transportowy, port docelowy, tagi, nagłówek syslog) i umożliwić wyszukiwanie wszystkich zapisanych logów w oparciu o te dane. Metadane powinny być dodawane do logu automatycznie nawet jeżeli nie został on poddany parsowaniu.

Alerty i korelacje

44 System musi być w stanie wygenerować alert jeżeli w procesowanym logu zostaną spełnione zdefiniowane warunki.

45 Alert musi być możliwy do wysłania poprzez wiadomość email, a jego treść możliwa do utworzenia przez użytkownika. System musi umożliwiać wykorzystanie pól procesowanego logu do tworzenia treści wiadomość email.

46 System musi być wyposażony w alerty i korelacje utworzone przez producenta.

47 System musi umożliwiać tworzenie alertów i korelacji poprzez wykorzystanie programowania wizualnego. Podobnie jak w przypadku tworzenia parserów musi istnieć

możliwość weryfikacji poprawności utworzonej logiki poprzez wykorzystanie testowego logu w oknie tworzenia alertu, oraz powiadamiania o ewentualnych błędach. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia i testowania poprawności alertu.

48 System musi umożliwiać wysłanie logu naruszającego zdefiniowaną logikę alertu do zewnętrznych systemów, co najmniej za pomocą protokołu SMPT lub Syslog (TCP). System musi umożliwiać definiowanie własnego formatu przesyłanego logu w celu łatwiejszego dostosowania go (integracji) do systemu docelowego. Wymagane jest dostarczenie dokumentacji opisującej ten proces.

49 System musi umożliwiać nie tylko wykorzystanie istniejących tagów, ale również nadawanie alertom nowych tagów. Wymagane jest dostarczenie dokumentacji opisującej sposób korzystania z gotowych tagów oraz przypisywania nowych.

50 System musi wspierać podstawowe funkcje SIEM - tworzenie tzw. korelacji zdarzeń, umożliwiających wygenerowanie alertu w przypadku przekroczenia określonego limitu lub wystąpienia kilku zdarzeń w zdefiniowanym oknie czasowym. Tworzenie i edycja reguł korelacji musi być możliwa do przeprowadzenia za pomocą interfejsu programowania graficznego wyposażonego w funkcjonalność sprawdzania działania logiki reguły na przykładowych logach.

Minimalne parametry sprzętowe oferowanego systemu

51 Pojedyncze urządzenie o rozmiarze max 1U, wyposażone w ramie do kabli umożliwiające wysunięcie urządzenia z szafy rack na potrzeby serwisowe bez konieczności wyłączania.

52 Urządzenie musi posiadać wszystkie komponenty niezbędne do działania (CPU, RAM, Dyski) i być niezależne od innych systemów.

53 1 procesor (min. 10 rdzeni) wspierający HyperThreading.

54 Min. 64GB DDR-4 RAM.

55 Przynajmniej 12TB przestrzeni dyskowej, wspieranej przez sprzętowy akcelerator SAS RAID. Kontroler macierzy dyskowej musi być wyposażony w zapasową baterię lub pamięć flash.

56 Z powodów wydajnościowych urządzenie musi być wyposażone w przynajmniej 4 dyski edycji RAID do wykorzystania w warunkach data center, o minimalnej prędkości 7200 rpm.

57 Przynajmniej 4 porty 1Gbit LAN + 1 dedykowany 1Gbit porty do zarządzania sprzętem. Konfiguracja parametrów wszystkich interfejsów sieciowych (w tym LACP) musi odbywać się z interfejsu graficznego web oraz musi być szczegółowo opisana w dokumentacji.

58 Wentylatory urządzenia muszą być wymienialne w trakcie pracy urządzenia i być redundantne.

59 Urządzenie musi być wyposażone w 2 źródła zasilania z redundancją 1+1.

60 Urządzenie musi wspierać Virtual KVM (keyboard,video,mouse).

61 Urządzenie musi wspierać zdalne zarządzanie oraz być dostarczone z licencją odpowiedniego typu (np.: iLO, iDRAC etc).

Wydajność oraz parametry oprogramowania systemu

62 System musi być dostarczony w formie urządzenia fizycznego (wszystkie elementy systemu

muszą być ustawialne z interfejsu graficznego web, bez konieczności edytowania żadnych plików systemowych, skryptów lub makr).

63 Aktualizacje systemu muszą być dystrybuowane w formie pojedynczego pliku i instalowane za pośrednictwem interfejsu graficznego web. Wszystkie aktualizacje muszą być możliwe do zainstalowania bez wsparcia dostawcy/producenta. Wymagamy dostarczenia przynajmniej 4 ostatnich dokumentów release notes w celu zweryfikowania proponowanych parametrów systemu.

64 System musi umożliwiać cofnięcie do poprzedniej wersji oprogramowania w przypadku wystąpienia problemów z działaniem po aktualizacji. Operacja musi być możliwa do wykonania bez wsparcia dostawcy/producenta. Wymagamy dostarczenia szczegółowego opisu procedury.

65 **System musi zapewnić średnią stałą wydajność procesowania min. 2 tysięcy logów na sekundę (2000 EPS), przy założeniu średniego rozmiaru logu równego 700 Bajtów.**

66 **W przypadku wystąpienia większej chwilowej ilości logów na sekundę, system musi być w stanie wykorzystać bufor i umożliwić odbieranie min. 4 tysiące logów na sekundę (4000 EPS) przez przynajmniej 10 minut.**

67 **Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie, lub licencja musi umożliwiać odbieranie przynajmniej 200GB logów/dzień. System musi posiadać bazę danych o rozmiarze przynajmniej 12TB oraz wspierać kompresję przechowywanych danych.**

68 System musi umożliwiać wzbogacanie logów o dodatkowe informacje z zewnętrznych list (przykład: wzbogacenie nazwy użytkownika o jego adres email i przynależność do grup AD).

69 System musi umożliwiać tagowanie indywidualnych źródeł danych, aplikacji, urządzeń czy całych podsieci IP, w celu oznaczania, przykładowo, lokalizacji urządzenia, jego typu, krytyczności etc.

70 Tagi muszą być możliwe do dodania w procesie tworzenia parsera.

71 Wszystkie dodane tagi muszą być przechowywane razem z logiem zapisanym w bazie. System musi umożliwiać filtrowanie i wyszukiwanie logów w oparciu o tagi, a także umożliwiać ograniczenie widoczności logów posiadających określony tag w procesie definiowania ról.

72 System musi umożliwiać wdrożenie w trybie wysokiej dostępności, w którym możliwe jest klastrowanie przynajmniej 2 urządzeń, widzianych i zarządzanych jako pojedyncza instancja. Ustawienia klastra muszą być możliwe do skonfigurowania przez interfejs graficzny web, nie jest dopuszczalne konfigurowanie klastra poprzez ręczne modyfikowanie plików systemu operacyjnego. System musi dostarczać użytkownikom czytelnych informacji o stanie klastra i synchronizacji bazy. Wymagamy dostarczenia dokumentacji opisującej cały proces tworzenia klastra, oraz odzyskiwania danych w przypadku awarii jednego z komponentów klastra.

73 Urządzenia pracujące w klastrze muszą przyśpieszać wyszukiwanie poprzez równoległe współdzielenie obciążenia.

74 W przypadku pracy w trybie wysokiej dostępności, źródła wysyłające dane muszą

wykorzystywać pojedynczy adres wirtualny, a klaster musi synchronizować konfigurację i odbierane logi pomiędzy urządzeniami w klastrze.

75 System musi wspierać tworzenie i odzyskiwanie kopii zapasowej konfiguracji. Wymagane jest dostarczenie dokumentacji opisującej ten proces.

76 System musi umożliwiać tworzenie i odzyskiwanie kopii zapasowej bazy danych. Tworzenie kopii zapasowej musi być możliwe zarówno na żądanie jak i w określonych interwałach czasowych. Tworzenie i odzyskiwanie musi być możliwe do wykonania z poziomu interfejsu graficznego web, bez konieczności tworzenia/modyfikowania skryptów, makr lub plików systemu operacyjnego. Wymagane jest dostarczenie dokumentacji opisującej ten proces.

Kolekcjonowanie zdarzeń z systemów Windows

77 Zdarzenia z systemów Windows muszą być zbierane przez dedykowane oprogramowanie (tzw. agent) instalowane bezpośrednio na stacjach końcowych i wysyłane do centralnej instancji systemu. Agent Windows musi umożliwiać zbieranie logów zarówno z systemowego dziennika zdarzeń jak i z plików testowych w systemie Windows. Wymagane jest dostarczenie dokumentacji opisującej działanie i konfigurację agenta.

78 Agent musi zapewniać zbieranie całych zdarzeń w niezmodyfikowanej formie (tzn. Nie tylko części zdarzenia).

79 System musi umożliwiać filtrowanie zdarzeń (przykładowo odrzucanie nieistotnych) zbieranych przez agenta Windows jeszcze przed wysłaniem do centralnej instancji.

80 Filtrowanie zdarzeń zbieranych przez agenta Windows musi być możliwe do skonfigurowania za pomocą programowania wizualnego. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia filtrów.

81 Agent Windows nie może wymagać interwencji administratora na systemie końcowym - musi być centralnie zarządzany, a jego konfiguracja możliwa do przeprowadzenia z poziomu interfejsu graficznego web, bez konieczności ręcznego edytowania plików systemowych. Konfiguracja agenta musi być automatycznie dystrybuowana bezpośrednio z centralnej konsoli systemu. Aktualizacje agenta nie mogą być przeprowadzane przy wykorzystaniu Group Policy w systemie Windows. Wymagane jest dostarczenie dokumentacji opisującej proces instalacji i konfiguracji agenta.

82 Agent Windows musi automatycznie tłumaczyć kody zdarzeń Windows na wiadomości tekstowe (przykładowo, Logon Type 2 = Interactive, Logon Type 3 = Network, etc.).

83 Agent Windows musi posiadać bufor na wypadek utraty połączenia stacji na której jest zainstalowany z centralną instancją systemu.

84 Komunikacja pomiędzy agentem Windows a centralną instancją systemu musi być zaszyfrowana, min. TLS 1.2.

85 Agent Windows musi wspierać kolekcjonowanie nie tylko podstawowych zdarzeń z dziennika zdarzeń (Application, Security, Setup, System) ale także umożliwiać zbieranie logów z folderu Applications and Services Logs. Dodatkowo, agent Windows musi umożliwiać pobierania plików tekstowych z systemu Windows, konfigurowane centralnie z poziomu interfejsu graficznego web, w tym możliwość wybrania ich formatu (przykładowo, txt, dhcp,

iis). Wymagane jest dostarczenie dokumentacji opisującej proces konfigurowania agenta.

86 Agent Windows musi automatycznie dodawać opis tekstowy do wszystkich zbieranych zdarzeń, dokładnie tak jak jest to prezentowane w Dzienniku Zdarzeń systemu Windows.

87 Agent Windows musi umożliwiać zbieranie logów z płaskich plików w systemie z którego zbierane są logi poprzez podanie ich ścieżki w systemie plików w menu konfiguracji agenta. Konfiguracja ścieżki musi uwzględniać wykorzystanie tzw. wildcardów (przykładowo: C\Windows\System32\dhcp\logs\Dhcp*.log - pobranie wszystkich plików z wskazanego folderu zaczynających się od "Dhcp" i kończących na ".log")

88 Musi istnieć możliwość zdalnego zatrzymania/uruchomienia usługi agenta na docelowym systemie - innymi słowy musi istnieć możliwość zmiany stanu odpowiedniej usługi z "Enabled" na "Disabled" i odwrotnie.

89 Agent musi automatycznie odpytywać centralny system w zadanym interwale - tzw. heartbeat - w celu sprawdzenia czy zaszły zmiany w konfiguracji - jeżeli tak to agent pobiera nową konfigurację, a następnie ją implementuje. Nie jest dopuszczalne "wypychanie" konfiguracji z centralnego systemu do agenta.

90 System musi posiadać wsparcie dla oprogramowania Elastic Beats - innymi słowy system musi umożliwiać zbieranie logów wysyłanych przez agenty Beats (filebeat/winlogbeat/auditbeat/metricbeat itd).

91 **Wymagamy minimum licencji na 50 systemów.**

Kolekcjonowanie zdarzeń ze zdalnych lokalizacji

92 System musi posiadać rozwiązanie umożliwiające zbieranie logów ze zdalnych lokalizacji i wysyłanie ich przez wysycony kanał bez utraty danych i zapewniając ich poufność. Wymagane jest dostarczenie dokumentacji opisującej takie rozwiązanie oraz schemat przepływu danych.

93 System musi umożliwiać centralne zarządzanie rozwiązaniem do zbierania logów ze zdalnych lokalizacji.

94 Rozwiązanie musi być w stanie automatycznie zestawić połączenie z centralną instancją systemu oraz zapewnić szyfrowanie przesyłanych danych. W przypadku utraty połączenia pomiędzy lokalizacją zdalną a centralną instancją systemu, rozwiązanie musi automatycznie podejmować próby ponownego połączenia.

95 Rozwiązanie musi umożliwić centralne ustawienie QoS dla przesyłania logów.

96 Rozwiązanie musi być wyposażone w bufor o rozmiarze co najmniej 100GB aby na wypadek utraty połączenia z centralną instancją logi nie zostały utracone.

97 Rozwiązanie musi zapewnić średnią stałą wydajność przesyłania min. 5 tysięcy logów na sekundę (5000 EPS), przy założeniu średniego rozmiaru logu równego 700 Bajtów.

98 Rozwiązanie musi zapewnić wsparcie dla kolekcjonowania logów na identycznym zakresie portów TCP i UDP jak centralna instancja systemu.

99 Rozwiązanie musi być dostępne w formie urządzenia fizycznego bądź jako system wirtualny pod kontrolą Vmware ESXi lub Hyper-V.

100	Rozwiązanie musi być w stanie komunikować się z centralną instancją systemu nawet jeżeli sieć wykorzystuje NAT.
	Wysoka dostępność, Wsparcie producenta oraz Gwarancja na sprzęt
101	Wymagana jest możliwość wdrożenia systemu w Wysokiej Dostępności w przyszłości
102	Hardware - min. 5 lat gwarancji na sprzęt ze wsparciem on-site i gwarantowanym czasem odpowiedzi next business day od momentu zgłoszenia awarii.
103	System musi wpierać TSR (Technical Support Report) w celu diagnostyki systemu bez konieczności uzyskiwania zdalnego dostępu.
104	Software - Wsparcie producenta systemu na 1 rok. Wsparcie musi uwzględniać aktualizacje oprogramowania i parserów przynajmniej 3 razy w roku, usuwanie błędów, wsparcie telefoniczne i email z dostępem zdalnym
	Referencje
105	Wymagane jest przedstawienie przynajmniej 2 referencji oferowanego systemu