Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Dostawa i montaż redundantnego serwera usług (bazodanowego, zarządzania użytkownikami, systemami i sieciami) wraz z instalacją i wdrożeniem **- liczba sztuk: 1**

   Producent: .....

   Model: .....

   Procesor .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	Obudowa Rack z możliwością instalacji min. 16 dysków 2.5” U.2 wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.	
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 48 rdzeniowych. Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
Procesor	zainstalowane dwa min. 24-rdzeniowe procesory umożliwiające osiągnięcie wyniku min. 400 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	
RAM	Minimum 512GB pamięci DDR5	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 1 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 40Gb lub 100Gb Ethernet w standardzie SFP28 Karta SAS o przepustowości min. 12 Gb/s kompatybilna z dostarczaną biblioteką taśmową (pkt.5)	
Dyski twarde	Zainstalowane: 2x kompatybilne dyski NVMe U.2 lub U.3 o	

	pojemności min. 1,92TB w RAID1 4 dyski NVMe U.2. lub U.3. min. 7TB z możliwością konfiguracji w RAID.	
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający. min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.	
Wbudowane porty	4x USB, w tym min. 1 porty USB 3.0 2x port VGA (jeden na panelu przednim)	
Wentylatory	Redundantne, Hot-Plug	
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium	
System operacyjny/dodatkowe oprogramowanie	Licencja na serwerowy system operacyjny, w wersji najnowszej oferowanej przez producenta musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Dostarczona licencja powinna umożliwiać korzystanie z usług serwera przez 70 użytkowników. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) 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. 2) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 3) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu	

	operacyjnego. 4) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 5) 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). 6) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 7) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 8) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 9) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 10) 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. 11) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek,	

	urządzeń sieciowych, standardów USB, Plug&Play). 12) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 13) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 14) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 15) 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. 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) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 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) 16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 17) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS powinien mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; a) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji	

	serwera); b) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; c) możliwość podmontowania zdalnych wirtualnych napędów; d) wirtualną konsolę z dostępem do myszy, klawiatury; e) wsparcie dla IPv6; f) wsparcie dla dynamic DNS; g) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
Warunki gwarancji	Min. 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)	

	Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy/ producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.	

2. Dostawa zasilaczy awaryjnych UPS stanowiskowych wraz z instalacją - liczba sztuk: 10

Producent: .....

Model: .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	desktop	
Typ	Line-interactive	
Tryb przebiegu pracy	Sinusoidalny	
Moc aktywna	800VA	
Porty komunikacyjne	Wbudowane porty komunikacyjne USB i/lub RS232 z programową obsługą sygnałów	
Zabezpieczenia	przeciwzwarciowe, przeciążeniowe, termiczne	
Certyfikaty	Zasilacz awaryjny UPS musi posiadać deklaracja CE	

Gwarancja producenta	Min. 2 lata	

3. Dostawa zasilaczy awaryjnych UPS serwerowych wraz z instalacją - liczba sztuk: 3

Producent: .....

Model: .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	Brak ograniczeń dot. obudowy	
Typ	Line-interactive	
Tryb przebiegu pracy	Sinusoidalny	
Moc aktywna	8000VA	
Porty komunikacyjne	Wbudowane porty komunikacyjne USB i/lub RS232 z programową obsługą sygnałów	
Zabezpieczenia	przeciwzwarciowe, przeciążeniowe, termiczne	
Instalacja	Wymagana instalacja niezbędnego okablowania i konfiguracja	
Certyfikaty	Zasilacz awaryjny UPS musi posiadać deklaracja CE	
Gwarancja producenta	Min. 2 lata	

4. Dostawa dysków do przechowywania kopii zapasowych - liczba sztuk: 6

Producent: .....

Model: .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Pojemność dysku	Min. 8TB	
Interfejs	SATA III	
Pamięć podręczna	Cache, min. 256MB	

Deklarowany MTBF	Min. 1mln godzin	
Technologia zapisu	Conventional Magnetic Recording (CMR)	
Parametry dodatkowe	Dedykowany do pracy 24h/7dni Zoptymalizowany do pracy w konfiguracjach RAID w środowiskach wielokieszeniowych	
Gwarancja producenta	Min. 5 lat	

5. Dostawa i wdrożenie biblioteki taśmowej wraz z nośnikami i z systemem automatyzacji kopii zapasowych – 1 zestaw

Dostawa automatycznej ładowarki taśmowej wraz z zestawem min. 9 taśm LTO-9, przeznaczonych do tworzenia kopii zapasowych i archiwizacji danych w środowisku IT. Rozwiązanie ma zapewniać wysoką niezawodność, łatwość zarządzania oraz zgodność z nowoczesnymi standardami przechowywania danych, wraz z systemem automatyzacji kopii zapasowych, jego wdrożeniem i konfiguracją, obejmującą automatyczną retencyjną i przyrostową kopie zapasowe baz danych, systemów dziedzinowych i plików serwerowych oraz użytkowników według wskazanego przez Zamawiającego harmonogramu.

Producent: .....

Model: .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Typ urządzenia	Automatyczna ładowarka taśmowa w obudowie rack o wysokości max 4U	
Napęd taśmowy	LTO-9, interfejs SAS (Serial Attached SCSI)	
Pojemność biblioteki	Obsługa do 9 kaset LTO-9 w wymiennym magazynku	
Zarządzanie	– Panel sterowania operatora z wyświetlaczem LCD umożliwiającym monitorowanie stanu urządzenia, diagnostykę, konfigurację oraz zarządzanie systemem. – Zdalne zarządzanie przez interfejs sieciowy (WWW) z dostępem za pośrednictwem przeglądarki	–

	internetowej	
Zgodność	Obsługa systemów operacyjnych Windows i Linux.	
Funkcjonalności	– Obsługa systemów operacyjnych Windows i Linux. – Automatyczne, nienadzorowane tworzenie kopii zapasowych. – Możliwość szybkiego dodawania/usuwania kaset dzięki stacji we/wy. – Obsługa szyfrowania sprzętowego oraz funkcji WORM (Write Once, Read Many). – Kompatybilność wsteczna z taśmami LTO-8 (odczyt i zapis).	–
Licencja na system	Licencja na system nieograniczona ilościowo i czasowo	
W zestawie	– Biblioteka taśmowa – 9 kaset LTO-9 – Kabel SAS min. 2m, o interfejsie min. 12Gb/s kompatybilny z kontrolerem serwera bazodanowego (pkt.1)	–
Gwarancja	Min. 5 lat w formie On-Site z czasem reakcji 1 dzień roboczy	

6. Dostawa i instalacja przełączników sieciowych - liczba sztuk: 6

Producent: .....

Model: .....

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	rack 19” o wysokości max. 2U	
Liczba i rodzaj portów	48x RJ45 min. 1Gb/s, min. 4 porty SFP+ 10Gb/s	
Przepustowość przełączania	min. 100Gbps	

Obsługiwane standardy	ANSI/TIA-1057:, IEEE 802.1AB, IEEE 802.1D, IEEE 802.1S, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1X, IEEE 802.3ac, IEEE 802.3ad, IEEE 802.3x	
Obsługiwane funkcjonalności	Port Security, co najmniej: Centralizowana konfiguracja VLAN, Spanning Tree, IGMP Snooping, L3 Routing, Virtual Domain, Policy-Based Routing, 802.1X Authentication, Obsługa Syslog, DHCP Snooping, MAC Filtering, Clients Monitoring, Application Control, sFlow, ACL, DHCP Relay, Port Mirroring, ECMP, BFD, WoL, zabezpieczenie przeciwko pętli, IGMP Snooping, Storm Control, Obsługa SNMP v3, RMON	
Zarządzanie	Telnet, SSH, HTTPs	
Praca w warstwach	L2, L3	
Certyfikaty	Przełącznik sieciowy musi posiadać deklaracja CE	
Gwarancja producenta	Min. 2 lata	

7. Dostawa i wdrożenie serwera logów systemowych, sieciowych oraz stacji roboczych

Producent serwera: ……
Model: ……

Producent oprogramowania do zbierania i analizy logów: ……
Nazwa i wersja: ……..

Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry techniczne
Obudowa	Obudowa Rack o wysokości max. 2U z możliwością instalacji min. 8 dysków 2.5” SATA/SSD wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.	
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji	

	pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
Procesor	zainstalowane dwa min. 12-rdzeniowe procesory umożliwiające osiągnięcie wyniku min. 200 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	
RAM	Minimum 64GB	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 1 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP28	
Dyski twarde	Zainstalowane: 2x kompatybilne dyski 2.5” SSD o pojemności min. 1,92TB skonfigurowane do pracy w trybie Mirror	
Wbudowane porty	4x USB, w tym min. 1 porty USB 3.0 2x port VGA (jeden na panelu przednim)	
Wentylatory	Redundantne, Hot-Plug	
Zasilacze	Redundantne, Hot-Plug min. 700W klasy Titanium	
Wraz z instalacją serwera wymagane jest wdrożenie oprogramowania do zbierania i analizy logów sieciowych, serwerowych i stacji końcowych obejmujących wymagania	– Centralny serwer logów uruchomiony w środowisku wirtualnym klasy Linux z dostępem do zarządzania za pomocą przeglądarki internetowej z aktywnym certyfikatem SSL. – Wymagana instalacja agentów na stanowiskach roboczych, pracujących pod kontrolą systemów operacyjnych: Windows 10/11, Windows Server 2022/2025, Linux Debian/Ubuntu (łącznie 96 sztuk) – System powinien umożliwiać zbieranie logów w zakresie co najmniej: – Logów zdarzeń systemu, w tym m.in.: o informacje, ostrzeżenia i błędy generowane przez aplikacje. o zdarzenia związane z komponentami systemu operacyjnego. o zdarzenia dotyczące bezpieczeństwa, takie jak logowania, zmiany uprawnień, próby	–

	dostępu nieautoryzowanego. o informacje o instalacjach i aktualizacjach systemu. – Monitorowania integralności, w tym, m.in.: o Wykrywanie zmian w krytycznych plikach systemowych, katalogach i plikach konfiguracyjnych. o Śledzenie modyfikacji, tworzenia i usuwania plików, co może wskazywać na aktywność złośliwego oprogramowania lub nieautoryzowane działania. – Monitorowanie rejestru systemu, w tym m.in. (dotyczy OS z rodziny Microsoft): o Śledzenie zmian w kluczach i wartościach rejestru. o Wykrywanie prób modyfikacji ustawień systemowych lub aplikacji. – Informacje o procesach i usługach, w tym m.in.: o Monitorowanie uruchomionych procesów i usług. o Wykrywanie uruchomienia nieznanych lub podejrzanych aplikacji. o Wykrywanie nieautoryzowanych instalacji lub zmian w konfiguracji sprzętowej. o Analiza systemu pod kątem obecności ukrytych procesów, modułów kernelowych i innych oznak infekcji. – Logi z zapory ogniowej i programów antywirusowych, w tym m.in.: o Zbieranie zdarzeń z Windows Defender, zapory ogniowej Windows i innych narzędzi zabezpieczających. o Monitorowanie prób włamań, blokowanych połączeń i wykrytych zagrożeń. – Monitorowanie sieci, w tym m.in.: o Zbieranie informacji o aktywnych połączeniach sieciowych. o Śledzenie otwartych portów i aktywności sieciowej.	

	– System powinien umożliwiać wizualizację i analizę danych, wyszukiwanie, archiwizację oraz monitorowanie i raportowanie w formie graficznej. – Na serwerze powinny być przechowywane logi z urządzeń UTM – Czas przechowywania wszystkich logów: min. 2 lata	
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS powinien mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; a) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); b) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; c) możliwość podmontowania zdalnych wirtualnych napędów; d) wirtualną konsolę z dostępem do	

	myszy, klawiatury; e) wsparcie dla IPv6; f) wsparcie dla dynamic DNS; g) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE.	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
Warunki gwarancji	Min. 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy/ producenta z właściwym	

	zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.	

8. Wdrożenie usługi katalogowej do centralnego zarządzania użytkownikami i uprawnieniami do systemów teleinformatycznych, synchronizacja stanowisk, konfiguracja polityk bezpieczeństwa

Zamawiający wymaga:

1. Konfiguracji i wdrożenia usługi katalogowej Active Directory w oparciu o Microsoft Windows Server 2025
2. Konfiguracji 90 stanowisk roboczych wg specyfikacji dostarczonej przez zamawiającego zawierającej:
    1. nazwę komputera,
    2. dane konta administratora lokalnego,
    3. nazwy i wersje aplikacji, które mają zostać zainstalowane (np. Adobe Reader, klient poczty, itp.).
    4. konfiguracja stacji roboczej i podłączenie jej do kontrolera AD,
    5. nadanie adresu IP odpowiedniego dla wydzielonej sieci VLAN.
    6. Utworzenie kont użytkowników i nadanie grup i uprawnień
    7. Utworzenie kompleksowe reguł polityk zabezpieczeń oraz pełne wdrożenie dla każdej z grup użytkowników reguł polityk Group Policy wraz z szablonami administracyjnymi (ok. 200 rekordów dla każdej grupy)
    8. migrację danych istniejących użytkowników z każdego stanowiska
3. konfiguracja urządzeń peryferyjnych: drukarki, skanery, itp.
    - nadanie nowego adresu IP odpowiedniego dla wydzielonej sieci VLAN,
    - nadanie lub zmianę istniejących haseł dostępowych,
    - zmianę ich konfiguracji celem wyeliminowania protokołów i ustawień mających wpływ na bezpieczeństwo danych.
4. Zamawiający nie dopuszcza możliwości realizowania zadanie zdalnie.

9. Wdrożenie polityk Port Security (DHCP Snooping, VLAN, DNS Spoofing, itd.) wraz z segmentacją sieci LAN i mapą sieci

1. Wdrożenie VLAN w strukturach sieci LAN – polegającym na odseparowaniu od siebie poszczególnych wydziałów z zachowaniem dostępności do urządzeń drukujących (urządzenia MFP w odrębnej sieci VLAN) oraz wydzielenia logicznego aktywnych urządzeń sieciowych, serwerowych i administracyjnych

2. Konfiguracja przełączników i wdrożenie polityki Port Security, w tym:
   - Uruchomienie protokołu MSTP oraz wdrożenie podsieci VLAN zgodnie ze wskazaniami Zamawiającego na wszystkich przełącznikach sieciowych
   - Konfiguracja protokołów służących do zdalnego zarządzania przełącznikami: SSH, HTTPS, SNMP
   - Zabezpieczenie wszystkich portów dostępowych z wykorzystaniem mechanizmów Port Security wskazanych przez Zamawiającego (w tym m.in. Broadcast/Multicast/Unknown Unicast Storm Recovery, DHCP Snooping, ARP Spooning, Port MAC Locking, Protected Ports, VLAN, QoS, ACL
   - zabezpieczenie przed nadmiernym ruchem broadcast-owym na portach dostępowych, w przypadku przekroczenia zdefiniowanych progów, ruch powinien być ograniczony lub port powinien zostać wyłączony.
   - należy skonfigurować protokół SNMP w celu monitoringu/zarządzania przełącznikami
   - ruch SNMP należy ograniczyć wyłącznie z/do serwerów monitorujących sieć i urządzenia
   - czas na przełącznikach należy synchronizować z serwerem czasu wskazanym przez Zamawiającego
3. Wykonanie mapy sieci obejmującej:
   - lokalizację
   - MAC adres i nazwę hosta podłączonego urządzenia
   - Synchronizację przepustowości i zmierzoną przepustowość trasy
   - Wskazanie konfiguracji VLAN dla portu
   - Wskazanie połączeń kaskadowych
4. Zamawiający nie dopuszcza możliwości realizowania zadanie zdalnie.

10. Wdrożenie usługi replikacji i synchronizacji danych serwera głównego z serwerem zapasowym zapewniającej nadmiarową kopię bezpieczeństwa

Zamawiający wymaga wykonania usługi polegającej na:

1. Uruchomienia środowiska wirtualizacji z opcją redundancji serwerowej i przeniesienia do tego środowiska istniejących serwerów fizycznych dla sieci Starostwa
2. Konfiguracji migracji serwerów, tak aby serwer zapasowy był zasilany w godzinach nocnych danymi serwera głównego.
3. Wdrożenie mechanizmu pozwalającego na sporządzanie danych w trybie tzw. kopii offline umożliwiającą wdrożenie retencji danych (np. tworzenie kopii na dyskach zewnętrznych umożliwiające ich codzienną wymianę)
4. Licencja systemu wirtualizacji i hosta dla systemu nie powinna być ograniczona czasowo i powinna generować kosztów licencji w przyszłości.
5. Zamawiający nie dopuszcza możliwości realizowania zadanie zdalnie.

11. Konfiguracja polityk VPN, aktualizacja i rekonfiguracja UTM, synchronizacja z usługami katalogowymi AD

Zamawiający wymaga wykonania usługi obejmującej skonfigurowanie polityk VPN, aktualizacja i rekonfiguracja urządzenia UTM (Unified Threat Management) oraz zapewnienie synchronizacji z usługami katalogowymi Active Directory (AD) w środowisku Windows 11. Zadanie ma na celu zapewnienie bezpiecznego zdalnego dostępu do zasobów sieciowych, optymalizację zabezpieczeń sieci oraz integrację z istniejącym systemem uwierzytelniania użytkowników.
Minimalne wymagania techniczne:

1. W ramach konfiguracji polityk VPN
   - Typ VPN: Skonfigurowanie bezpiecznego tunelu VPN opartego na protokole IPsec lub SSL, w zależności od wymagań środowiska.
   - Uwierzytelnianie: Wdrożenie uwierzytelniania wieloskładnikowego (MFA) z integracją z Active Directory (AD) dla użytkowników Windows 11.
   - Utworzenie zasad dostępu VPN dla różnych grup użytkowników (np. pracownicy, administratorzy) z uwzględnieniem ograniczeń dostępu do określonych zasobów sieciowych.
   - Definicja reguł dla split tunneling lub pełnego tunelowania, w zależności od potrzeb bezpieczeństwa.
   - Bezpieczeństwo: Wdrożenie szyfrowania AES-256, konfiguracja zapory sieciowej (firewall) dla ruchu VPN oraz zapewnienie ochrony przed atakami typu man-in-the-middle.
   - Kompatybilność: Zapewnienie wsparcia dla klientów VPN na systemie Windows 11, w tym natywnego klienta Windows oraz dedykowanego oprogramowania VPN Forticlient
2. Aktualizacja i rekonfiguracja UTM Fortigate
   - Przegląd i optymalizacja istniejących reguł zapory sieciowej (firewall), filtrów URL oraz polityk IPS (Intrusion Prevention System).
   - Konfiguracja ochrony przed zagrożeniami, w tym antywirus, antyspam i ochrona przed atakami DDoS.
   - Monitorowanie i logowanie: Skonfigurowanie logowania zdarzeń bezpieczeństwa oraz integracja z systemem SIEM dla monitorowania w czasie rzeczywistym.
   - Wydajność: Optymalizacja ustawień UTM w celu minimalizacji opóźnień i zapewnienia wysokiej przepustowości dla ruchu sieciowego.
3. Synchronizacja z usługami katalogowymi Active Directory (Windows 11)
   - Integracja z AD: Skonfigurowanie synchronizacji urządzenia UTM i serwera VPN z usługami katalogowymi Active Directory w środowisku Windows 11.
   - Uwierzytelnianie użytkowników: Wdrożenie protokołu LDAP lub Kerberos dla uwierzytelniania użytkowników VPN i dostępu do zasobów sieciowych na podstawie grup AD.
   - Automatyzacja przypisywania uprawnień na podstawie członkostwa w grupach AD.
   - Synchronizacja atrybutów użytkowników (np. nazwy, role) między AD a urządzeniem UTM/VPN.

- Testowanie: Weryfikacja poprawności synchronizacji poprzez testy logowania użytkowników z różnych grup AD na urządzeniach z systemem Windows 11.

4. Dokumentacja:
   - Dostarczenie pełnej dokumentacji konfiguracyjnej w języku polskim lub angielskim, obejmującej schematy sieci, polityki VPN, ustawienia UTM oraz procedury synchronizacji z AD.
5. Zamawiający nie dopuszcza możliwości realizowania zadanie zdalnie.

12. Dostawa i wdrożenie systemu antywirusowego dla serwerów, stacji roboczych i urządzeń mobilnych wraz z mechanizmami piaskownicy

Producent: .....
Nazwa i wersja: .....

Dostawa licencji na system zabezpieczający przed złośliwym oprogramowaniem dla 90 sztuk stacji roboczych, 40 urządzeń mobilnych oraz 6 serwerów na okres maksymalnie do 20 maja 2026 r. oraz wdrożenie i konfiguracja na każdym urządzeniu. Zamawiający nie dopuszcza możliwości realizacji wdrożenia zdalnie.

Parametry i funkcjonalności dostarczonego Systemu, nie mogą być gorsze niż wskazane poniżej:

1. System musi zapewniać ochronę antywirusową:
   - serwera plików,
   - stacji roboczych,
   - urządzeń przenośnych (smartfony, tablety),
2. Dla stacji roboczych system musi ponadto zapewnić kontrolę podłączanych urządzeń (np. pamięci USB, zewnętrzne napędy, itp.).
3. Konfiguracja, nadzór nad pracą poszczególnych modułów oraz instalacja na stacjach roboczych winna być wykonywana z centralnej webowej konsoli zarządzającej dostarczonej w ramach przedmiotu zamówienia przez Wykonawcę.
4. Wsparcie techniczne powinno odbywać się w języku polskim przez cały czas trwania umowy (jako serwis telefoniczny bądź za pomocą poczty elektronicznej).
5. Moduł ochrony antywirusowej, antispyware i ransomware musi poprawnie współpracować z następującymi systemami operacyjnymi wykorzystywanymi przez Zamawiającego: Microsoft Windows, Linux i macOS.
6. Moduł ochrony stacji roboczych musi posiadać polskojęzyczny interfejs i zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
7. Moduł ochrony antywirusowej musi: realizować ochronę na podstawie:
   - sygnatur,
   - heurystyki (z możliwością jej wyłączenia),

- na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet;
- posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony;
- umożliwiać skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu z następującymi warunkami:
- skanowanie na żądanie i według harmonogramu mieć możliwość przerwania w dowolnym momencie,
- skanowanie na żądanie z możliwością wstrzymania w przypadku wykrycia pracy na baterii lub w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja);
- wykrywać zagrożenia: na dyskach, w plikach w tym archiwach plikowych, na stronach web, w przesyłkach e-mail w tym w załącznikach, na podłączanych nośnikach przenośnych;
- zapewniać ochronę komunikacji przy wykorzystaniu protokołów POP3, SMTP w czasie rzeczywistym niezależnie od klienta pocztowego;
- zapewniać ochronę komunikacji przy wykorzystaniu protokołu HTTP w czasie rzeczywistym niezależnie od przeglądarki;
- zawierać programy (plugin-y do przeglądarek Microsoft IE, Mozilla Firefox i Google Chrome) działające na stacjach użytkowników i ostrzegające ich o złośliwej zawartości strony internetowej wraz z możliwością aktywnego blokowania dostępu do wybranych stron internetowych, określonych centralnie przez administratora systemu.
- Rozwiązanie musi realizować także możliwość określenia blokowanych stron web na podstawie kategorii strony (np. pornografia, strony społecznościowe, itp.) lub moduł musi umożliwiać blokowanie stron na podstawie predefiniowanych kategorii oraz konkretnych adresów URL, w określonych przez administratora przedziałach czasu;
- umożliwiać ustawienia priorytetu procesu skanowania;
- realizować aktualizację wzorców wirusów musi odbywać się co najmniej raz dziennie;
- umożliwiać aktualizację wzorców wirusów z archiwum internetowego lub z centralnego punktu dystrybucji wzorców wirusów;
- mieć możliwość pobierania aktualizacji za pośrednictwem serwera Proxy;
- po wykryciu zagrożenia posiadać możliwość oczyszczenia zainfekowanego pliku, a jeśli nie jest to możliwe – usunięcia bądź umieszczenia go w lokalnej kwarantannie;
- umożliwiać konfigurowanie dostępności i zakresu ingerencji użytkownika w proces skanowania;
- pozwolić na zabezpieczanie hasłem przed zmianą konfiguracji, deinstalacją i zatrzymaniem programu;
- wymuszać odświeżanie wzorców wirusów;
- uaktualniać silnik oprogramowania i bazy wzorców wirusów przez cały okres trwania umowy.
- Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych

protokołów HTTPS, RDP, FTPS, SCP/SSH.

8. Moduł ochrony urządzeń mobilnych.
   - Ochronę urządzeń pracujących pod kontrolą wykorzystywanych przez Zamawiającego systemów Android oraz Apple iOS.
   - Ochronę plików w czasie rzeczywistym.
   - Skanowanie plików systemowych, bibliotek, plików archiwum oraz innych.
   - Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
   - Ochronę proaktywną wykrywającą nieznane zagrożenia.
   - Określenie poziomu głębokości skanowania plików archiwum.
   - Określenie domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
   - W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
   - Włączenie blokady urządzenia mobilnego na hasło alfanumeryczne o zadanej złożoności: np. minimum 8 znaków składających się z liter małych i dużych, oraz cyfr i znaków specjalnych.
   - Ustalenie czasu, po którym włącza się blokada urządzenia (np. blokada ekranu po 5 minutach nieaktywności użytkownika).
   - Pamięć historii haseł blokady urządzenia, wykluczająca możliwość użycia co najmniej 5 ostatnich haseł.
   - Możliwość wykrywania ingerencji w oryginalne oprogramowanie urządzenia.
   - Możliwość blokowania aplikacji po jej nazwie.
   - Możliwość zarządzania dedykowaną konsolą on-line.
9. Moduł centralnej konsoli zarządzającej musi:
   - zapewnić centralną instalację programów służących do ochrony stacji roboczych Windows oraz urządzeń mobilnych na OS Android;
   - zapewnić centralne zarządzanie wszystkimi programami służącymi do ochrony: stacji roboczych, serwerów plików, urządzeń mobilnych;
   - posiadać centralną bazę przechowującą informacje o konfiguracji stacji i urządzeń końcowych;
   - posiadać centralną bazę przechowującą informacje o zdarzeniach i wykrytych zagrożeniach;
   - umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów;
   - Możliwość przechowywania kwarantanny do 180 dni.
   - Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.

- szkolenie dla administratora z zakresu obsługi, konfiguracji i administracji dostarczonego rozwiązania.

10. Zamawiający nie dopuszcza możliwości realizowania wdrożenia zdalnie.

13. Wdrożenie mechanizmów wykrywania incydentów i automatycznego reagowania XDR wraz z wdrożeniem szyfrowania dla 90 stacji roboczych.

Producent: .....
Nazwa i wersja: .....

Zamawiający wymaga wykonania usługi polegającej na wdrożeniu systemu XDR (Extended Detection and Response) zapewniającego monitorowanie, wykrywanie incydentów bezpieczeństwa, automatyczne reagowanie oraz zgodność z regulacjami. Zamówienie obejmuje również wdrożenie szyfrowania 90 stacjach roboczych z systemem Windows 11 oraz 6 serwerach Windows Server oraz Linux w celu ochrony danych.

Minimalne wymagania techniczne:

1. Instalacja i konfiguracja usługi serwera centralnego:
   - Wdrożenie serwera XDR na systemie Linux (64-bit) w lokalnym środowisku wirtualnym
   - Konfiguracja komponentów: zarządzania zdarzeniami, indeksowania danych, interfejsu użytkownika (dashboard).
   - Zapewnienie wysokiej dostępności i skalowalności systemu dla obsługi 90 stacji roboczych oraz 6 serwerów
2. Wdrożenie agentów na stacjach roboczych:
   - Instalacja agentów XDR na 90 stacjach z systemem Windows 11 oraz 6 serwerach Windows Server oraz Linux.
   - Konfiguracja agentów do zbierania logów systemowych, monitorowania integralności plików, skanowania podatności oraz analizy behawioralnej.
3. Funkcjonalności XDR:
   - Monitorowanie w czasie rzeczywistym zdarzeń bezpieczeństwa, w tym logów systemowych, aplikacji i sieci.
   - Automatyczna korelacja danych z punktów końcowych, sieci i chmury w celu wykrywania zagrożeń.
   - Wykrywanie incydentów, takich jak złośliwe oprogramowanie, ransomware, nieautoryzowany dostęp, z wykorzystaniem ram takich jak MITRE ATT&CK.
   - Automatyczne reakcje na incydenty, np. izolacja stacji roboczych, blokowanie adresów IP, terminowanie procesów.
   - Generowanie dashboardów i raportów dla audytów bezpieczeństwa.
   - Możliwość integracji z systemami SOAR dla zaawansowanej automatyzacji reakcji
   - Integracja z narzędziami do szczegółowego monitorowania zdarzeń na stacjach Windows
   - Generowanie raportów zgodności i audytów bezpieczeństwa.

4. Wdrożenie usługi szyfrowania:
   - Wdrożenie natywnego szyfrowania (np. BitLocker) na 90 stacjach roboczych z systemem Windows 11 Professional
   - Konfiguracja szyfrowania pełnego dysku z algorytmem AES-256 i zarządzaniem kluczami odzyskiwania.
   - Integracja z Active Directory dla centralnego zarządzania kluczami.
   - Konfiguracja systemu XDR do monitorowania stanu szyfrowania na stacjach roboczych.
   - Generowanie alertów w przypadku prób nieautoryzowanego dostępu lub zmiany statusu szyfrowania.
5. Szkolenia i dokumentacja:
   - Przeprowadzenie szkolenia stacjonarnego dla zespołu IT z zakresu konfiguracji, zarządzania i reagowania na incydenty w systemie XDR.
   - Szkolenie z zarządzania mechanizmem szyfrowania.
   - Przygotowanie szczegółowej dokumentacji wdrożeniowej, obejmującej konfigurację serwera, agentów, reguł reagowania oraz procedury zarządzania szyfrowaniem, Instrukcje zmiany haseł administracyjnych i aktualizacji systemu.

14. Dostawa i wdrożenie systemu do inwentaryzacji zasobów sieci, urządzeń sieciowych, drukarek i urządzeń drukujących oraz serwerów i jednostek komputerowych

Producent: .....
Nazwa i wersja: .....

Dostawa i wdrożenie na każdej stacji roboczej (90szt), przełączniku sieciowym (8szt), sieciowych urządzeniach drukujących (40szt) specjalistycznego oprogramowania zapewniającego:

1. monitoring stacji roboczych, serwerów, urządzeń drukujących, urządzeń sieciowych,
2. rozliczalność zgłoszeń, rozwiązywania awarii itp.,
3. zarządzanie użytkownikami,
4. zarządzanie zasobami IT

Spełniającego minimalnie wymagania:

- System umożliwiający monitorowanie sieci, urządzeń sieciowych, drukarek i urządzeń drukujących, jednostek komputerowych, nośników pamięci.
- Licencja do 20 maja 2026 r. dla 90 stacji roboczych i 6 serwerów
- Kompleksowe wdrożenie systemu wraz z instalacją na 90 stacjach roboczych i 6 serwerach w siedzibie Zamawiającego oraz szkoleniem dla administratorów.
- Oprogramowanie musi posiadać polski interfejs językowy.
- Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
- Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.

- Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
- Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
- Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
- Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
- Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów
  obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
- Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności
  użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
- Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline)
- Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.
- Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
- Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
- Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
- Oprogramowanie musi umożliwiać analizę sprzętową:
  - płyty głównej w zakresie model, producent, nr. Seryjny,
  - CPU w zakresie nazwy, modelu, producenta, częstotliwości,
  - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
  - RAM w zakresie wielkości pamięci,
  - karty sieciowej w zakresie model, adres IP, adres MAC,
  - karty graficznej w zakresie model.
- Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
- Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
- Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
- Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
- Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

- Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
- Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
- Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
- Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
- Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
- Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
- Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
- Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
- Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
- Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.
- Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa.
- Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
- Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę mobilną umożliwiającą spis z natury zinwentaryzowanych zasobów.
- Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
- Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
- Oprogramowanie musi umożliwiać zdalne zarządzanie lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
- Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
- Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
- Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
- Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

- Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
- Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
- Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
- Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
- Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
- Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD z parametrami do każdej akcji
- Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
- Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
- Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
- Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
- Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
- Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
- Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
- Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD o Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
- Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.

- Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
- Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
- Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).
- Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:
  - Zarządzanie problemem
  - Zarządzanie incydentem
  - Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
  - Zarządzanie umowami serwisowymi
  - Definicje poziomów SLA (reakcja, naprawa, reklamacja)
  - Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki
  - WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
  - Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
  - Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
  - Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
  - Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
  - Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
- `Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
- Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupiony sprzętem.
- Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
- Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, itd.
- Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.

- Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
- Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
- Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
- Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym suportem producenta, liczonym od daty zakończenia wdrożenia, maksymalnie do 20 maja 2026 r.
- Zamawiający nie dopuszcza możliwości realizowania wdrożenia zdalnie.

UWAGA: ZAMAWIAJĄCY WYMAGA UZUPEŁNIENIA PARAMETRÓW WE WSKAZANYCH MIEJSCACH W KOLUMNIE ***Oferowane parametry techniczne.*** BRAK UZUPEŁNIENIA WYMAGANYCH PARAMETRÓW I/LUB DANYCH BĘDZIE SKUTKOWAŁO ODRZUCENIEM OFERTY

Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym