

Wnioskodawca:

Michał Kirsztling – Kierownik Działu Infrastruktury Sportowej

OPIS PRZEDMIOTU ZAMÓWIENIA

(zamówienia wieloasortymentowe dla dostaw – w zależności od specyfikacji zamówienia można zastosować własny formularz)

I. Nazwa zadania: Dostawa, montaż i konfiguracja elementów systemu IT (serwer, oprogramowanie do monitoringu, oprogramowanie do zarządzania i monitorowania IT)

1. Przedmiot zamówienia część 1:

Dostawa, montaż i konfiguracja serwera NAS wraz z dyskami pamięci i systemem do zarządzania i monitorowania IT

2. Wymagania ogólne:

Przedmiotem zamówienia jest dostawa, montaż i kompleksowa konfiguracja fabrycznie nowego serwera NAS wraz z 12 dyskami klasy Enterprise o pojemności 12 TB każdy (technologia CMR) oraz wdrożenie zaawansowanej platformy do zarządzania i monitorowania IT.

Wykonawca musi przeprowadzić wszystkie prace zgodnie z rygorystycznymi standardami bezpieczeństwa środowiska informatycznego Zamawiającego (dokument do wglądu u Zamawiającego), gwarantując najwyższy poziom ochrony i stabilności przetwarzanych danych

Zakończenie prac wymaga dostarczenia kompletnej dokumentacji powykonawczej, zawierającej topologię logiczną sieci, tablicę adresacji, rejestr ryzyk oraz sformalizowane procedury awaryjne.

Wszystkie dostarczane urządzenia, podzespoły oraz oprogramowanie muszą być fabrycznie nowe, nieużywane, kompletne i gotowe do natychmiastowej eksploatacji.

Zarówno serwer NAS, jak i wszystkie dyski twarde muszą zostać wyprodukowane nie wcześniej niż w roku poprzedzającym ich dostawę do Zamawiającego.

Wymagane jest, aby oferowane dyski twarde oraz wszelkie dodatkowe moduły oraz akcesoria pochodziły od tego samego producenta co jednostka centralna serwera NAS, co gwarantuje pełną kompatybilność sprzętową.

Całość rozwiązania musi zapewniać maksymalny poziom bezpieczeństwa przechowywanych danych oraz gwarantować stabilną pracę w trybie ciągłym.

Do pracy w infrastrukturze Zamawiającego dopuszcza się wyłącznie urządzenia posiadające aktywne i pełne wsparcie techniczne producenta.

Sprzęt musi pochodzić z oficjalnego i autoryzowanego kanału sprzedaży na rynek europejski, zapewniając pełną ochronę gwarancyjną i dostęp do aktualizacji firmware.

Oprogramowanie klasy Enterprise musi być dostarczone w najnowszej stabilnej wersji, umożliwiając pełną kontrolę nad infrastrukturą i bezpieczeństwem.

Wykonawca dostarczy urządzenia w nienaruszonych opakowaniach fabrycznych, zawierających komplet akcesoriów, szyny montażowe oraz instrukcje obsługi.

3. Wymagania (parametry) szczegółowe w wersji tabelarycznej:

Lp.	Asortyment	J.m.	Ilość	Opis wymagań minimalnych	Uzasadnienie wymagań
1	2	3	4	5	6
1	Serwer NAS	szt.	1	Procesor: minimum Intel Xeon D-1541	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Liczba procesorów: minimum 1	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Liczba rdzeni procesora: minimum 8	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Liczba wątków procesora: minimum 16	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Architektura procesora: 64-bity	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Częstotliwość procesora: minimum 2.1 GHz podstawowo, minimum 2.7 GHz w trybie turbo	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Mechanizm szyfrowania sprzętowego: Tak	Wskazany parametr zapewni maksymalne bezpieczeństwo danych
				Wbudowana pamięć systemowa: minimum 16 GB DDR4 ECC UDIMM, tego samego producenta co Serwer NAS	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Rozbudowa pamięci urządzenia do 128 GB GB DDR4 ECC UDIMM, tego samego producenta co Serwer NAS	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Całkowita liczba gniazd pamięci: minimum 4	Wskazany parametr zapewni płynną i bezproblemową pracę urządzenia
				Ilość kieszeni na dysk: minimum 12	Wskazany parametr zapewni odpowiednią ilość miejsca na dane
				Zgodność dysków: 3,5" SATA HDD, 2,5" SATA HDD, Dysk SATA SSD 2,5"	Wskazany parametr zapewni ograniczenie zużycia energii
				Funkcja hot-swap: Tak	Parametr ten zapewni nieprzerwaną pracę w przypadku awarii dysku
				Porty zewnętrzne: minimum 4x RJ-45 1GbE, minimum 2x USB 3.2 1. Generacji, minimum 2x RJ-45 10GbE	Wskazane parametry pozwalają zwiększyć funkcjonalność urządzenia
				Dodatkowe złącze PCIe: minimum 2x Gen3 x8 slots (x8 link)	Wskazane parametry pozwalają zwiększyć funkcjonalność urządzenia
				Typ obudowy: 2U	Wskazany parametr pozwoli na umieszczenie w istniejącej infrastrukturze
				Rozmiary(wys. x szer. x gł.): maksymalnie 88 x 485 x 725 mm	Wskazany parametr pozwoli na umieszczenie w istniejącej infrastrukturze
				Waga bez dysków: Maksymalnie 14,5 kg	Wskazany parametr pozwoli na umieszczenie w istniejącej infrastrukturze
				Wentylatory w obudowie: minimum 4 sztuki 80x80mm każdy	Wskazany parametr zapewni odpowiednie chłodzenie w każdych warunkach

				Tryby pracy wentylatora: pełnej prędkości, chłodzenia i cichy	Wskazany parametr zapewni odpowiednie chłodzenie w każdych warunkach
				Natężenie dźwięku: maksymalnie 50.5 dB	Wskazany parametr zapewni maksymalne bezpieczeństwo danych znajdujących się dysku
				Zużycie energii: maksymalnie 140 W w trybie dostępu oraz maksymalnie 59 W w trybie hibernacji dysków twardych	Wskazany parametr zapewni ograniczenie zużycia energii
	Oprogramowanie systemu NAS	kpl.	1	Obsługa typów macierzy minimum: RAID 0, RAID 1, RAID5, RAID 6, RAID 10, RAID F1, Basic, JBOD	Wskazany parametr pozwoli na konfigurację najbardziej dopasowaną do odbiorcy
				Maksymalna liczba wolumenów wew: minimum 256	Wskazany parametr pozwoli na konfigurację najbardziej dopasowaną do odbiorcy
				Obsługa funkcji SSD TRIM	Parametr ten pozwoli na zaoszczędzenie miejsca na urządzeniu
				Integracja listy kontroli dostępu systemu Windows (ACL)	Parametr ten pozwala na zachowanie zgodności uprawnień plików z systemami Windows oraz umożliwia centralne zarządzanie dostępem do zasobów
				Uwierzytelnienie NFS Kerberos	Parametr ten zwiększa poziom bezpieczeństwa
				Obsługiwane systemy plików: Minimum Btrfs, ext4 – dla dysków wewnętrznych Btrfs, ext4, ext3, Fat32, NTFS, HFS+, exFAT dla dysków zewnętrznych	Parametr ten zapewnia kompatybilność z różnorodnymi nośnikami danych oraz systemami operacyjnymi
				Obsługiwane protokoły plików minimum: SMB, AFP, NFS, FTP, WebDAV, Rsync	Parametr ten pozwala na integrację urządzenia z różnymi środowiskami systemowymi i aplikacyjnymi
				Maksymalna możliwa liczba folderów udostępnionych: minimum 512	Parametr ten pozwala na tworzenie dużej liczby zasobów sieciowych dla wielu użytkowników, projektów lub aplikacji
				Maksymalna liczba zadań synchronizacji folderów udostępnionych: minimum 12	Parametr ten pozwala na synchronizację wielu lokalizacji danych pomiędzy systemami lub lokalizacjami
				Maksymalna liczba folderów Hybrid Share: minimum 15	Parametr ten pozwala na integrację i współdzielenie zasobów pomiędzy infrastrukturą lokalną a środowiskiem chmurowym
				Dostępne oprogramowanie wykonujące backup wskazanych folderów, plików lub całych maszyn	Parametr ten zapewnia możliwość kompleksowego zabezpieczenia danych oraz systemów w ramach jednej platformy
				Wspierana wirtualizacja: ESXi 8.0 U2, ESXi 8.0 U1, ESXi 8.0, ESXi 7.0 U3, ESXi 7.0 U2, ESXi 7.0 U1, ESXi 7.0, ESXi 6.7 U3, ESXi 6.7 U2, ESXi 6.7 U1, ESXi 6.7, ESXi 6.5 U3, ESXi 6.5 U2, ESXi 6.5 U1, ESXi 6.5,	Parametr ten zapewnia kompatybilność z różnymi środowiskami informatycznymi
				Maksymalna liczba jednoczesnych zadań pobierania: minimum 80	Parametr ten umożliwia obsługę wielu równoległych

					operacji pobierania danych bez istotnego wpływu na wydajność systemu
				Maksymalna liczba celów iSCSI: minimum 128	Parametr ten pozwala na udostępnienie wielu wirtualnych zasobów dyskowych dla serwerów i środowisk wirtualnych
				Obsługa migawek	Parametr ten pozwala na zwiększenie bezpieczeństwa danych
				Maksymalna liczba migawek na folder udostępniony: minimum 256	Parametr ten pozwala na zwiększenie bezpieczeństwa danych
				Maksymalna liczba migawek na system: minimum 16,384	Parametr ten pozwala na zwiększenie bezpieczeństwa danych
	Wypożyczenie	kpl.	1	- kabel zasilający - instrukcja	Wypożyczenie niezbędne do podłączenia serwera.
	Gwarancja	Miesiąc e	Min. 36	Min. 36 miesięcy na serwer oraz oprogramowanie	Gwarancja zapewniająca, długotrwałą bezawaryjną pracę
	Dysk twardy	szt.	12	Rozmiar dysku: minimum 12 TB	Wskazany parametr zapewni odpowiednią ilość miejsca na dane
				Rodzaj obudowy: 3.5"	Wskazany parametr zapewni kompatybilność z serwerem NAS
				Interfejs: SATA 6 Gb/s	Wskazany parametr zapewni bardzo dobrą prędkość zapisywania i odczytywania danych
				Rozmiar sektora: minimum 512e	Wskazany parametr zapewni bardzo dobrą prędkość zapisywania i odczytywania danych
				Prędkość obrotowa: minimum 7,200 rpm	Wskazany parametr zapewni bardzo dobrą prędkość zapisywania i odczytywania danych
				Szybkość interfejsu: minimum 6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s	Wskazany parametr zapewni bardzo dobrą prędkość zapisywania i odczytywania danych
				Rozmiar buforu: minimum 256 MiB	Wskazany parametr zapewni bardzo dobrą prędkość zapisywania i odczytywania danych
				Maksymalna stała prędkość przesyłu danych: minimum 242 MiB/s	Wskazany parametr zapewni bardzo dobrą prędkość zapisywania i odczytywania danych
				Średni czas do awarii (MTTF): minimum 2.5 mln godzin	Wskazany parametr zapewni maksymalne bezpieczeństwo danych znajdujących się dysku
				Ocena obciążenia: minimum 550 TB przeniesionych danych rocznie	Wskazany parametr zapewni maksymalne bezpieczeństwo danych znajdujących się dysku
				Zużycie energii podczas aktywnego trybu bezczynności: maksymalnie 4.30W	Wskazany parametr zapewni ograniczenie zużycia energii
				Zużycie energii podczas losowego odczytu/zapisu (4 KB Q1): maksymalnie 7.90W	Wskazany parametr zapewni ograniczenie zużycia energii

3	Karta Rozszerzeń	szt.	Min. 36	Odporność na wstrząs: minimum 686 m/s ² {70 G} (czas trwania 2 ms)	Wskazany parametr zapewni maksymalne bezpieczeństwo danych znajdujących się dysku
				Rozmiar (wys. x szer. x gł.): maksymalnie 26.1 mm x 101.85 mm x 147 mm	Wskazany parametr zapewni kompatybilność z serwerem NAS
				Waga: maksymalnie 720 g	Wskazany parametr zapewni kompatybilność z serwerem NAS
	Gwarancja	miesiąc	Min. 36	Min. 36 miesięcy na dyski twarde	Gwarancja zapewniająca, długotrwałą bezawaryjną pracę
				Interfejs magistrali: minimum 1 x PCIe 3.0 x8	Parametr zapewni odpowiednią przepustowość
				Rozmiar: maksymalnie 70 mm x 170 mm x 15mm	Parametr pozwoli na bezproblemowy montaż karty w urządzeniu
				Zgodność ze specyfikacją minimum: IEEE 802.3x, IEEE 802.3ad Link Aggregation, Gigabitowy Ethernet IEEE 802,3ab, IEEE 802.3an 10 Gb/s Ethernet	Parametr gwarantuje i kompatybilność z istniejącą infrastrukturą sieciową oraz możliwość wykorzystania standardowych mechanizmów zarządzania ruchem.
				Szybkość transmisji danych: minimum 10 Gbps/1 Gbps	Parametr ten umożliwia szybszy transfer danych
				Obsługa mechanizmu TCP Segmentation Offload (TSO)	Pozwala na odciążenie procesora hosta poprzez realizację segmentacji pakietów TCP na poziomie sprzętowym.
				Obsługa mechanizmu Receive Side Scaling (RSS)	Pozwala na równoważenie obciążenia ruchu sieciowego pomiędzy wieloma rdzeniami procesora.
				Obsługa mechanizmu Generic Segmentation Offload (GSO)	Wspomaga segmentowanie dużych pakietów danych.
				Obsługa ramek Jumbo Frame w zakresie co najmniej od 1,5 KB do 9 KB	Parametr ten pozwala zwiększyć efektywność transmisji w sieciach o dużej przepustowości.
				Obsługa sprzętowego odciążania obliczania sum kontrolnych dla protokołów TCP oraz UDP (TCP/UDP Checksum Offload).	Parametr ten pozwala zmniejszyć obciążenie procesora
				Obsługa mechanizmu Transmit Side Scaling (TSS)	Parametr ten pozwala na rozłożenie operacji wysyłania pakietów pomiędzy wiele kolejek i rdzeni procesora, zwiększając wydajność transmisji wychodzącej.
				Obsługa technologii SR-IOV (Single Root I/O Virtualization)	Parametr ten pozwala na efektywną wirtualizację interfejsu sieciowego i bezpośredni dostęp maszyn wirtualnych do zasobów sprzętowych.
				Obsługa mechanizmu Large Receive Offload (LRO)	Parametr ten pozwala na zmniejszenie liczby operacji przetwarzanych przez system
	Gwarancja	Miesiąc	Min. 36	Min. 36 miesięcy na kartę rozszerzeń	Gwarancja zapewniająca długotrwałą bezawaryjną pracę

4	Szyny montażowe Nazwa produktu	kpl.	1	Wymagana szerokość podstawy stelaża min. 450 mm	Parametr pozwalający montaż serwera w szafie Zamawiającego.
				Wymagana szerokość panela min. 480 mm	Parametr pozwalający montaż serwera w szafie Zamawiającego.
				Wymagana głębokość montażu na stelażu: min. 610 mm - max 890 mm	Parametr pozwalający montaż serwera w szafie Zamawiającego.
				Obsługa otworów montażowych stelaży: otwory kwadratowe: min. 9.5 mm x 9.5 mm otwory okrągłe: min. 7.1 mm	Parametr pozwalający montaż serwera w szafie Zamawiającego.
5	Pamięć DDR 4 ECC RDIMM	kpl.	1	Min. 128 GB DDR 4 ECC Registered DIMM	Wskazany parametr zagwarantuje odpowiednią wydajność i ciągłość pracy systemu
	Gwarancja	miesiąc y	Min. 36	Min. 36 miesięcy na pamięci ram	Gwarancja zapewniająca długotrwałą bezawaryjną pracę
6	Systemem do zarządzania i monitorowania IT	kpl.	1	System musi umożliwić bezproblemową i stabilną obsługę co najmniej 80 Klientów.	Wskazany parametr zagwarantuje odpowiednią wydajność i ciągłość pracy systemu przy docelowej wielkości środowiska Zamawiającego.
				Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.	Wymóg ten gwarantuje ciągły i bezpieczny nadzór nad stacjami roboczymi w tle, bez zakłócania bieżącej pracy użytkowników.
				Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).	Wymóg ten zapewni administratorom elastyczny i zdalny dostęp do zarządzania systemem z poziomu przeglądarki internetowej, bez konieczności instalacji dodatkowego oprogramowania na ich stacjach roboczych.
				Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.	Wymóg ten zapewni wygodną komunikację na linii pracownik-administrator oraz sprawny dostęp do niezbędnych informacji bez konieczności dodatkowego uwierzytelniania.
				Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.	Wymóg ten zagwarantuje scentralizowane i niezawodne gromadzenie danych oraz zarządzanie wszystkimi monitorowanymi stacjami końcowymi.
				Baza danych pracująca na silniku Microsoft SQL Server w wersjach 2014/2016/2017/2019/2022 w wersji 64 bitowych wersja standard (Uwaga: licencje do Microsoft SQL Server należy dostarczyć osobno)	Wymóg ten zapewni optymalizację kosztów wdrożenia systemu przy jednoczesnym zagwarantowaniu wysokiej wydajności i kompatybilności ze standardowymi środowiskami bazodanowymi Zamawiającego.
				Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych)	Wymóg ten zapewni wysoki poziom bezpieczeństwa oraz bezobsługowe utrzymanie

			aktualizują się automatycznie poprzez bezpieczne połączenie.	całego systemu zawsze w najnowszej wersji.
			System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.	Wymóg ten zapewni optymalną wydajność systemu i odciąży administratorów dzięki cyklicznemu, bezobsługowemu wykonywaniu zadań utrzymaniowych.
			Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox)	Wymóg ten zapewni administratorom swobodny i czytelny dostęp do zarządzania systemem z poziomu dowolnego urządzenia, niezależnie od używanej przeglądarki internetowej.
			Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.	Wymóg ten zapewni możliwość objęcia jednolitym zarządzaniem i monitoringiem całej, zróżnicowanej infrastruktury sprzętowo-systemowej funkcjonującej u Zamawiającego.
			Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2	Wymóg ten gwarantuje rzetelne i kompletne zbieranie danych o aktywności internetowej pracowników w najpopularniejszych przeglądarkach wykorzystywanych w organizacji Zamawiającego.
			Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.	Wymóg ten zapewni pełną kompatybilność oprogramowania serwerowego z 64-bitowym środowiskiem operacyjnym Microsoft wykorzystywanym w infrastrukturze Zamawiającego.
			Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.	Wymóg ten gwarantuje kompatybilność i stabilne działanie serwera WWW w ramach ustandaryzowanego środowiska Zamawiającego, opartego o technologie Microsoft i Java.
			System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V VMWare oraz NASA	Wymóg ten zapewni dużą elastyczność wdrożenia oraz zagwarantuje prawidłowe działanie oprogramowania w oparciu o posiadane przez Zamawiającego zasoby wirtualizacyjne i sieciowe urządzenia pamięci masowej.
			System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury	Wymóg ten zautomatyzuje zarządzanie zasobami i wyeliminuje błędy ręcznego wprowadzania danych dzięki ściślejszej integracji z istniejącą usługą katalogową Zamawiającego.

				System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL	Wymóg ten zapewni łatwą migrację informacji oraz elastyczną integrację z różnorodnymi, popularnymi zewnętrznymi źródłami danych wykorzystywanymi przez Zamawiającego.
				System zapewnia integrację z modelem LLM.	Wymóg ten zapewni wsparcie administratorów w szybkiej analizie logów i rozwiązywaniu problemów dzięki wykorzystaniu zaawansowanych możliwości sztucznej inteligencji.
				System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika.	Wymóg ten zapewni administratorom pełną kontrolę nad stacjami roboczymi bez konieczności fizycznego dostępu oraz umożliwi skuteczną i w pełni rejestrowaną komunikację z użytkownikami.
				Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardsy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika.	Wymóg ten zagwarantuje administratorom kompleksowy, wielojęzyczny wgląd w stan całej infrastruktury i bezpieczeństwa dzięki zaawansowanej wizualizacji danych oraz szerokim możliwościom personalizacji interfejsu.
				W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.	Wymóg ten zapewni ergonomiczną pracę dostosowaną do indywidualnych potrzeb operatorów oraz zagwarantuje bezpieczeństwo systemu dzięki szczegółowej kontroli uprawnień zintegrowanej z usługą katalogową Zamawiającego.
				Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.	Wymóg ten znacząco usprawni pracę administratorów poprzez umożliwienie masowego wykonywania operacji oraz zagwarantuje szybką diagnozę dzięki dostępowi do precyzyjnych danych o podłączonych urządzeniach.
				Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.	Wymóg ten zapewni bezobsługowy i bezpieczny dostęp do narzędzi samoobsługowych i analitycznych dla pracowników oraz kadry kierowniczej, przy jednoczesnym zachowaniu przez administratorów pełnej kontroli nad zakresem udostępnianych informacji.

				System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji	Wymóg ten umożliwi Zamawiającemu pełną kontrolę nad legalnością i kosztami oprogramowania oraz zapewni bezpieczeństwo poprzez sprawną eliminację niepożądanych aplikacji.
				System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu	Wymóg ten zagwarantuje Zamawiającemu precyzyjną identyfikację i monitorowanie faktycznego wykorzystania aplikacji, co jest niezbędne do optymalizacji kosztów oraz rzetelnych audytów legalności.
				System musi posiadać zdolności do bieżąco i automatycznego identyfikowania podatności w zainstalowanym oprogramowaniu.	Wymóg ten zagwarantuje Zamawiającemu precyzyjną identyfikację i monitorowanie faktycznego wykorzystania aplikacji, co jest niezbędne do optymalizacji kosztów oraz rzetelnych audytów legalności.
				System musi posiadać zdolności do bieżąco i automatycznego identyfikowania podatności w zainstalowanym oprogramowaniu.	Wymóg ten umożliwi organizacji proaktywne wykrywanie luk bezpieczeństwa w infrastrukturze IT, co znacząco zminimalizuje ryzyko wystąpienia incydentów cybernetycznych i wycieków danych.
				System musi posiadać zdolności do bieżąco i automatycznego identyfikowania podatności w zainstalowanym oprogramowaniu.	Wymóg ten zagwarantuje Zamawiającemu precyzyjną identyfikację i monitorowanie faktycznego wykorzystania aplikacji, co jest niezbędne do optymalizacji kosztów oraz rzetelnych audytów legalności.
				Wykrywanie podatności musi być oparte o analizę wzorców zainstalowanego oprogramowania i porównanie ich z globalnymi bazami podatności, takimi jak CVE (Common Vulnerabilities and Exposures).	Oparcie analizy na uznanej, globalnej bazie CVE gwarantuje najwyższą wiarygodność i aktualność informacji o lukach bezpieczeństwa, umożliwiając skuteczną ochronę przed znanymi zagrożeniami.
				System powinien posiadać co najmniej dwa wskaźniki umożliwiające ocenę poziomu ryzyka i priorytetyzację zagrożeń.	Wymóg ten umożliwi administratorom obiektywną ocenę powagi wykrytych luk oraz efektywne planowanie działań naprawczych według ich priorytetu.
				System musi mieć możliwość ustawiania powiadomień o wykrytych podatnościach.	Funkcja ta zapewni bezzwłoczne informowanie administratorów o nowych zagrożeniach, umożliwiając błyskawiczną reakcję na krytyczne luki bezpieczeństwa.

				System musi mieć możliwość automatycznego tworzenia incydentów w przypadku integracji systemu z systemem eHelpDesk.	Automatyzacja przepływu informacji o awariach do systemu zgłoszeniowego skróci czas reakcji serwisu i usprawni proces zarządzania incydentami w organizacji.
				Powinna istnieć funkcja raportowania z możliwością filtrowania wg urządzenia, typu podatności lub poziomu krytyczności.	Wymóg ten umożliwi generowanie precyzyjnych zestawień analitycznych, co jest kluczowe dla sprawnego zarządzania procesem usuwania luk oraz dostarczania rzetelnych danych do audytów bezpieczeństwa i kadry zarządzającej.
				System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian.	Wymóg ten umożliwi Zamawiającemu zachowanie pełnej kontroli nad posiadanymi zasobami sprzętowymi, ułatwi planowanie modernizacji (upgrade'ów) oraz pozwoli na szybkie wykrywanie nieautoryzowanych zmian w konfiguracji komputerów lub połączeń urządzeń zewnętrznych, co ma kluczowe znaczenie dla bezpieczeństwa fizycznego danych.
				System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia	Wymóg ten umożliwi uzyskanie pełnej i spójnej widzialności całej infrastruktury hybrydowej (fizycznej i wirtualnej) w jednym systemie. Automatyzacja wykrywania urządzeń oraz wizualizacja topologii sieci (mapy) są kluczowe dla szybkiej diagnostyki problemów komunikacyjnych i sprawnego zarządzania rozproszonym środowiskiem IT.
				System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach	Wymóg ten umożliwi objęcie ewidencją wszystkich zasobów IT w organizacji, a nie tylko stacji roboczych, co jest niezbędne do rzetelnego zarządzania majątkiem (Fixed Assets Management). Automatyczne przypomnienia o gwarancjach i umowach serwisowych pozwolą na uniknięcie nieplanowanych kosztów napraw oraz zapewnią ciągłość wsparcia technicznego dla kluczowych urządzeń infrastrukturalnych.
				Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych komercyjnej lub bezpłatnej (np. Microsoft SQL Server Express Edition).	Wymóg ten gwarantuje wykorzystanie stabilnego i wydajnego silnika bazy danych, który jest standardem w środowiskach korporacyjnych. Zapewnia to

					<p>bezpieczeństwo danych, wysoką dostępność oraz łatwość backupu.</p> <p>Dopuszczenie wersji bezpłatnej (Express) pozwala na optymalizację kosztów wdrożenia przy zachowaniu pełnej funkcjonalności systemu w mniejszych środowiskach.</p>
				<p>System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.</p>	<p>Wymóg ten jest kluczowy dla zapewnienia skutecznej ochrony informacji o znaczeniu strategicznym, tajemnic handlowych oraz danych osobowych przetwarzanych w organizacji. Możliwość blokowania niepożądanych działań w czasie rzeczywistym pozwala na natychmiastowe przeciwdziałanie incydentom, zanim dojdzie do nieodwracalnego wycieku danych, co zapewnia zgodność z normami bezpieczeństwa i przepisami prawa (np. RODO).</p>
				<p>System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.</p>	<p>Wymóg ten ma na celu wyeliminowanie „czynnika ludzkiego” i opóźnień w reagowaniu na zagrożenia. Automatyczne uruchamianie ochrony w czasie rzeczywistym gwarantuje, że zasoby organizacji są zabezpieczone od pierwszej sekundy pojawienia się w sieci, a egzekwowanie polityk odbywa się bez przerwy, co drastycznie skraca czas ekspozycji na potencjalne incydenty bezpieczeństwa.</p>
				<p>System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).</p>	<p>W dobie pracy hybrydowej i mobilnej, tradycyjna ochrona oparta na obwodzie sieci (firewallu) jest niewystarczająca. Wymóg ten gwarantuje, że polityki bezpieczeństwa i mechanizmy ochrony danych (DLP) są aktywne bezpośrednio na stacji roboczej, zapewniając bezpieczeństwo informacji również wtedy, gdy pracownik korzysta z publicznych sieci Wi-Fi, domowego łącza bez zestawionego tunelu VPN czy pracuje w trybie offline.</p>
				<p>System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.</p>	<p>Wymóg ten zapewnia pełną skalowalność systemu oraz możliwość precyzyjnego dostosowania ochrony do specyfiki różnych działów w organizacji (np. HR, Finanse,</p>

					IT). Brak ograniczeń w liczbie reguł pozwala na budowanie złożonych i wielopoziomowych scenariuszy ochrony danych, co jest niezbędne dla zachowania zgodności z dynamicznie zmieniającymi się regulacjami prawnymi (np. RODO) oraz wewnętrznymi standardami bezpieczeństwa bez konieczności dokupowania dodatkowych modułów przy rozbudowie polityk.
				System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.	Wymóg ten zapewnia administratorom niezbędną elastyczność w zarządzaniu bezpieczeństwem, umożliwiając szybkie reagowanie na sytuacje wyjątkowe (np. specyficzne, jednorazowe procesy biznesowe) oraz ułatwia diagnostykę i dostrajanie systemu. Możliwość wyłączenia reguły zamiast jej usuwania pozwala na zachowanie wypracowanych konfiguracji i szybki powrót do pełnej ochrony bez ryzyka popełnienia błędów przy ponownym definiowaniu parametrów.
				System musi w pełni wspierać następujące polityki ochrony danych: Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione Wyświetlanie komunikatu na komputerach użytkowników.	Wymóg ten gwarantuje utrzymanie wysokiego poziomu higieny cyfrowej w organizacji poprzez ścisłą kontrolę nad zainstalowanymi aplikacjami. Automatyzacja usuwania zabronionego oprogramowania drastycznie zmniejsza ryzyko infekcji malware oraz naruszeń licencyjnych bez angażowania personelu IT. Z kolei zaawansowany system komunikatów startowych jest niezbędny do skutecznego budowania świadomości bezpieczeństwa (security awareness) oraz sprawnego informowania pracowników o planowanych przerwach technicznych czy procedurach alarmowych w sposób czytelny i profesjonalny.
				System musi blokować dostęp do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzeń USB. (REMOVABLE DEVICE)	Wymóg ten jest kluczowy dla zabezpieczenia stacji roboczych przed nieautoryzowanym wypływem danych (DLP) oraz ryzykiem infekcji złośliwym oprogramowaniem (np. typu Ransomware) przenoszonym

					na pendrive'ach. Precyzyjne zarządzanie dostępem do portów USB pozwala na zachowanie ciągłości procesów biznesowych (np. korzystanie z autoryzowanych kluczy sprzętowych) przy jednoczesnym wyeliminowaniu zagrożenia ze strony prywatnych, niezaufanych nośników danych.
				System umożliwia zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www. (WEB)	Wprowadzenie kontroli dostępu do zasobów internetowych jest niezbędne dla zapewnienia wysokiej produktywności pracowników oraz ochrony sieci przed zagrożeniami typu phishing czy malware, często dystrybuowanymi za pośrednictwem mediów społecznościowych lub niezaufanych blogów. Możliwość kategoryzacji stron pozwala administratorom na elastyczne dopasowanie polityki dostępu do potrzeb poszczególnych działów, co optymalizuje wykorzystanie pasma internetowego i minimalizuje ryzyko naruszeń bezpieczeństwa cyfrowego.
				System umożliwia blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych. (WLAN)	Wymóg ten jest niezbędny dla zapewnienia integralności i bezpieczeństwa przesyłanych danych poprzez uniemożliwienie urządzeniom służbowym łączenia się z niezaufanymi lub publicznymi sieciami bezprzewodowymi (np. otwarte hotspoty, sieci domowe o niskim standardzie zabezpieczeń). Kontrola nad typem i nazwą (maską) sieci Wi-Fi minimalizuje ryzyko ataków typu <i>Man-in-the-Middle</i> oraz niekontrolowanego transferu danych poza bezpieczny obwód organizacji.
				System umożliwia wyświetlanie powiadomienia o przekroczeniu dozwolonego czasu pracy komputera. (WORKING TIME)	Wprowadzenie powiadomień o czasie pracy wspiera organizację w dbaniu o dobrostan pracowników (well-being) oraz ułatwia przestrzeganie przepisów BHP i prawa pracy dotyczących przerw. Z punktu widzenia technicznego, funkcja ta zachęca do regularnego restartowania urządzeń, co jest kluczowe dla poprawnej

					instalacji aktualizacji systemowych oraz czyszczenia pamięci tymczasowej, co bezpośrednio przekłada się na stabilność i wydajność infrastruktury.
				Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.	Wymóg ten jest niezbędny do uszczelnienia "analogowej" luki w bezpieczeństwie danych. Ponieważ nieautoryzowane nośniki USB stanowią jeden z najczęstszych wektorów wycieku informacji oraz infekcji złośliwym oprogramowaniem, system musi nie tylko blokować, ale i precyzyjnie audytować każde podłączone urządzenie. Posiadanie pełnej historii i klasyfikacji (np. odróżnienie myszki od pendrive'a) pozwala na prowadzenie skutecznych analiz śledczych (<i>forensic</i>) po wystąpieniu incydentu oraz na bezpieczne dopuszczenie do pracy wyłącznie zweryfikowanych urządzeń służbowych.
				System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS_AES_256 i AES_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/desyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.	Wymóg ten jest kluczowy dla zapewnienia najwyższego poziomu poufności danych przechowywanych na stacjach roboczych i nośnikach przenośnych, szczególnie w przypadku ich zgubienia lub kradzieży. Centralizacja kluczy odzyskiwania w konsoli administracyjnej eliminuje ryzyko trwałej utraty dostępu do danych przez organizację, a możliwość zarządzania procesem poza siecią lokalną (poza NAT) jest niezbędna w dobie pracy zdalnej. Wykorzystanie natywnego mechanizmu BitLocker przy jednoczesnym ukryciu procesu przed użytkownikiem końcowym gwarantuje bezpieczeństwo bez wpływu na komfort i ciągłość pracy.
				System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą	Wymóg ten jest fundamentem nowoczesnego i efektywnego wsparcia technicznego (Helpdesk) oraz administracji systemowej. Zdalne zarządzanie plikami, rejestrem i aplikacjami bez przerywania pracy użytkownika (tzw. praca w

				<p>technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.</p>	<p>tle) skraca czas rozwiązywania problemów. Wykorzystanie Intel vPro pozwala na interwencję nawet w przypadku awarii systemu operacyjnego (dostęp poza pasmem – out-of-band), co drastycznie redukuje koszty serwisowania w terenie. Dodatkowo, wsparcie AI w generowaniu skryptów minimalizuje ryzyko błędów ludzkich i pozwala na błyskawiczną automatyzację nowych, specyficznych zadań administracyjnych.</p>
				<p>System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.</p>	<p>Automatyzacja zarządzania poprawkami minimalizuje ryzyko cyberataków przy zachowaniu pełnej produktywności użytkowników dzięki dyskretnym instalacjom w tle. Funkcja wycofywania aktualizacji oraz zaawansowanego raportowania zapewnia administratorom pełną kontrolę nad stabilnością floty urządzeń i procesem skutecznego usuwania krytycznych podatności.</p>
				<p>System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.</p>	<p>Centralne zarządzanie zaporą sieciową gwarantuje spójność polityk bezpieczeństwa w całej organizacji i eliminuje ryzyko błędnych konfiguracji na poszczególnych stacjach roboczych. Monitorowanie stanu w czasie rzeczywistym pozwala na natychmiastowe wykrywanie i blokowanie incydentów sieciowych, co jest kluczowe dla ochrony przed rozprzestrzenianiem się zagrożeń wewnątrz infrastruktury.</p>
				<p>System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.</p>	<p>Precyzyjny harmonogram prac konserwacyjnych oraz automatyzacja procesów porządkowych gwarantują wysoką dostępność systemów i optymalną wydajność bazy danych przy minimalnym zaangażowaniu personelu technicznego. System wczesnego ostrzegania o brakach licencyjnych oraz nowych urządzeniach pozwala na bieżąco kontrolować legalność oprogramowania i błyskawicznie reagować na nieautoryzowane zmiany w infrastrukturze IT.</p>

				<p>Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.</p>	<p>Centralne repozytorium dokumentów w konsoli administracyjnej zapewnia błyskawiczny dostęp do instrukcji, licencji i faktur przypisanych bezpośrednio do zasobów IT, co znacząco usprawnia procesy audytowe i serwisowe. Możliwość tworzenia logicznych kontenerów pozwala na zachowanie strukturalnego porządku w dokumentacji, eliminując ryzyko rozproszenia kluczowych informacji technicznych wewnątrz organizacji.</p>
				<p>System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.</p>	<p>Wykorzystanie kodów jedno- i dwuwymiarowych drastycznie przyspiesza proces inwentaryzacji fizycznej oraz eliminuje błędy ludzkie podczas ręcznego wprowadzania danych o sprzęcie do bazy. Możliwość parametryzacji graficznej pozwala na precyzyjne dostosowanie etykiet do wymiarów różnych urządzeń oraz standardów identyfikacji wizualnej obowiązujących w organizacji.</p>
				<p>System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikiem a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji.</p>	<p>Bezpośredni komunikator skraca czas reakcji na incydenty techniczne i pozwala na błyskawiczne wyjaśnienie wątpliwości bez konieczności przełączania się między zewnętrznymi narzędziami takimi jak e-mail czy telefon. Centralna historia czatów stanowi cenne źródło wiedzy przy rozwiązywaniu powtarzających się problemów oraz zapewnia pełną dokumentację wsparcia udzielonego użytkownikowi końcowemu.</p>
				<p>System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.</p>	<p>Monitoring wydruków pozwala na precyzyjną kontrolę kosztów operacyjnych oraz identyfikację nieefektywnych nawyków w skali całej organizacji. Bieżący podgląd stanu materiałów eksploatacyjnych umożliwia proaktywne planowanie zakupów i serwisowania, co skutecznie eliminuje nagłe przestoje w pracy biurowej.</p>
				<p>System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https),</p>	<p>Monitorowanie zaszyfrowanego ruchu HTTPS przy wsparciu sztucznej inteligencji</p>

				<p>rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.</p>	<p>pozwala na precyzyjną identyfikację zagrożeń i naruszeń polityk bezpieczeństwa, które pozostają niewidoczne dla tradycyjnych narzędzi filtrujących. Dzięki zaawansowanej analizie treści możliwe jest skuteczne zapobieganie wyciekom danych oraz optymalizacja produktywności poprzez automatyczną klasyfikację odwiedzanych witryn.</p>
				<p>System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.</p>	<p>Bieżące monitorowanie dostępności i wydajności serwerów WWW pozwala na błyskawiczne wykrywanie awarii oraz optymalizację czasu odpowiedzi kluczowych usług biznesowych. Graficzna analiza trendów i treści stron umożliwia administratorom proaktywne zarządzanie infrastrukturą oraz szybką identyfikację anomalii w działaniu aplikacji sieciowych.</p>
				<p>System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.</p>	<p>Centralne monitorowanie dzienników zdarzeń pozwala na błyskawiczną identyfikację krytycznych błędów systemowych oraz prób nieautoryzowanego dostępu, zanim wpłyną one na ciągłość pracy organizacji. Dzięki zaawansowanemu filtrowaniu administratorzy mogą skutecznie przeprowadzać analizę przyczyn awarii i proaktywnie zarządzać stabilnością całej infrastruktury IT.</p>
				<p>System musi umożliwiać monitorowanie komunikatów Syslog.</p>	<p>Centralizacja komunikatów Syslog z urządzeń sieciowych i serwerów pozwala na błyskawiczną diagnostykę problemów infrastrukturalnych oraz wykrywanie incydentów bezpieczeństwa w jednym, spójnym panelu zarządzającym. Dzięki temu administratorzy mogą efektywnie monitorować stan urządzeń od różnych producentów, co znacząco skraca czas reakcji na awarie w heterogenicznych środowiskach IT.</p>
				<p>System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.</p>	<p>Monitorowanie czasu pracy oraz logowań użytkowników jest kluczowe dla zapewnienia bezpieczeństwa tożsamości cyfrowej oraz pełnej rozliczalności działań podejmowanych wewnątrz</p>

					infrastruktury IT. Widoczność szczegółów sesji połączeń wraz z adresami IP umożliwia administratorom błyskawiczną identyfikację anomalii oraz precyzyjne śledzenie zdarzeń w przypadku wystąpienia incydentów naruszenia ochrony danych.
				System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.	Monitorowanie uprawnień ACL jest niezbędne dla utrzymania zasady minimalnych uprawnień oraz ochrony poufnych danych przed nieautoryzowanym dostępem wewnątrz struktury organizacyjnej. Automatyczne skanowanie pozwala na błyskawiczne wykrywanie błędów w dziedziczeniu uprawnień oraz luk w zabezpieczeniach, które w rozbudowanych systemach plików mogłyby pozostać niezauważone.
				System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.	Monitorowanie parametrów środowiskowych przez SNMP pozwala na wczesne wykrywanie zagrożeń fizycznych, takich jak przegrzanie serwerowni czy awaria klimatyzacji, co bezpośrednio zapobiega kosztownym uszkodzeniom sprzętu i nieplanowanym przestojom. Dzięki graficznej analizie trendów oraz systemowi natychmiastowych alertów administratorzy mogą proaktywnie reagować na anomalie, zanim wpłyną one na stabilność i żywotność kluczowych elementów infrastruktury IT.
				System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach	Zintegrowana baza CMDB jest niezbędna do zachowania pełnej przejrzystości powiązań między użytkownikami, sprzętem a oprogramowaniem w ramach jednego, spójnego ekosystemu informacyjnego. Pozwala to na precyzyjne planowanie wydatków oraz błyskawiczną identyfikację zasobów podczas audytów legalności czy skomplikowanych procesów usuwania awarii.
				System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych	Precyzyjna analiza aktywności i czasu pracy pozwala na sprawiedliwą ocenę zaangażowania oraz optymalizację procesów wewnątrz zespołów bez

				<p>analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach</p>	<p>uciażliwego, ręcznego wypełniania arkuszy. Transparentne udostępnianie tych statystyk samym pracownikom w dedykowanym panelu wspiera ich autonomię i pozwala na lepsze zarządzanie własną produktywnością w oparciu o twarde dane.</p>
				<p>System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów.</p>	<p>Rozbudowany system raportowania z integracją dla profesjonalnych narzędzi takich jak Crystal Reports umożliwia przekształcenie surowych danych w precyzyjną analitykę biznesową dostosowaną do specyficznych potrzeb organizacji. Automatyzacja harmonogramów oraz szeroki wachlarz formatów eksportu eliminują konieczność ręcznego przygotowywania zestawień, gwarantując kadry zarządzającej stały dostęp do kluczowych wskaźników infrastruktury bez zbędnej zwłoki.</p>
				<p>System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON.</p>	<p>Udostępnienie nowoczesnego interfejsu REST API z szyfrowaniem TLS 1.3 zapewnia najwyższy standard bezpieczeństwa danych podczas integracji z zewnętrznymi systemami klasy korporacyjnej. Taka architektura pozwala na elastyczną automatyzację przepływu informacji za pomocą ustrukturyzowanych zapytań JSON przy jednoczesnej ochronie przed nieautoryzowanym dostępem.</p>
				<p>System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD</p>	<p>Wielokanałowy system powiadomień obejmujący alerty konsolowe, wiadomości e-mail oraz SMS zapewnia bezzwłoczny przepływ informacji o krytycznych zdarzeniach do odpowiednich grup decyzyjnych niezależnie od ich lokalizacji. Integracja z interfejsami CMD i Windows PowerShell pozwala na budowę zautomatyzowanych scenariuszy naprawczych, w których wykryty incydent automatycznie uruchamia dedykowany skrypt usuwający awarię bez udziału administratora.</p>

				System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania.	Wdrożenie wieloskładnikowego uwierzytelniania oraz restrykcyjnej polityki haseł drastycznie redukuje ryzyko nieautoryzowanego dostępu do konsoli zarządzającej w przypadku przejęcia danych logowania. Centralne zarządzanie uprawnieniami w połączeniu z szyfrowaniem danych zapewnia poufność informacji o infrastrukturze i gwarantuje pełną zgodność z rygorystycznymi standardami bezpieczeństwa IT.
				Pomoc techniczna Musi być świadczona 24 h 7 dni w tygodniu czas reakcji 4 godziny	Dostępność wsparcia technicznego w trybie 24/7 z gwarantowanym czteroosobowym czasem reakcji jest kluczowa dla zapewnienia nieprzerwanej ciągłości działania systemów o znaczeniu krytycznym dla organizacji. Taki rygor serwisowy pozwala na błyskawiczną neutralizację awarii i zagrożeń bezpieczeństwa, minimalizując potencjalne straty operacyjne wynikające z nieplanowanych przestojów infrastruktury.
				Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA)	Zapewnienie ciągłości działania oraz regularnych aktualizacji jest kluczowe dla zachowania wysokiego poziomu bezpieczeństwa i pełnej kompatybilności oprogramowania z dynamicznie zmieniającą się infrastrukturą IT. Profesjonalne wsparcie w ramach SLA minimalizuje ryzyko strat operacyjnych i gwarantuje szybki dostęp do eksperckiej wiedzy w przypadku wystąpienia nieprzewidzianych trudności technicznych.
				Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.	Roczny okres obowiązywania umowy SLA gwarantuje stabilność operacyjną oraz pełną przewidywalność kosztów utrzymania systemu w całym cyklu budżetowym organizacji. Zapewnia to stały dostęp do krytycznych aktualizacji i wsparcia eksperckiego, co jest niezbędne dla zachowania wysokiego poziomu bezpieczeństwa infrastruktury IT w kluczowym okresie jej eksploatacji.

7	<p>Usługi opisane w załączniku nr 5a do SWZ, w tym :</p> <p>Faza 1: Przygotowanie warstwy fizycznej i zasilania</p> <p>Faza 2: Konfiguracja sieciowa i segmentacja</p> <p>Faza 3: Warstwa składowania i wirtualizacji</p> <p>Faza 4: Implementacja Systemu Zarządzania i Monitorowania IT</p> <p>Faza 5: Backup, Dokumentacja i Testy</p> <p>Usługi wymagane w ramach serwisu gwarancji</p> <p>Inne usługi niezbędne do wykonania całości zamówienia w części 1 wymienione w opisie przedmiotu zamówienia w załączniku nr 5a, a nie wymienione powyżej</p>
---	--

4. Harmonogram i metodyka wdrożenia systemu NAS oraz platformy zarządzania IT:

Wdrożenie musi zostać przeprowadzone z rygorystycznymi normami bezpieczeństwa systemów teleinformatycznych. Proces podzielono na krytyczne fazy technologiczne. Konfiguracje należy przeprowadzić stacjonarnie u Zamawiającego.

Faza 1: Przygotowanie warstwy fizycznej i zasilania

- ☐ Montaż serwera (2U) + 12x HDD Enterprise CMR. Podpięcie zasilaczy do dwóch niezależnych PDU, Zamawiający posiada rozwiązania Schneider Electric, konfiguracja po SNMP.
- ☐ Przygotowanie instalacji pomiędzy dwoma serwerowniami, które są w osobnych lokalizacjach. Należy przewidzieć pracę tj spawanie światłowodu 4 włókien, instalacja okablowania CAT7 maksymalnie 30 metrów pomiędzy szafami dystrybucyjnymi.
- ☐ Inicjalizacja systemu. Wyłączenie domyślnego konta admin. Wymuszenie 2FA/MFA dla grupy Administrators.
- ☐ Czas: Konfiguracja klienta NTP i synchronizacja z serwerem czasu Zamawiającego.

Faza 2: Konfiguracja sieciowa i segmentacja

- ☐ Agregacja L2: Zestawienie LACP (IEEE 802.3ad) na portach 10GbE SFP+ do switchy rdzeniowych (przepustowość 20 Gbps). Zamawiający posiada rozwiązania Alcatel-Lucent Enterprise.
- ☐ Segmentacja VLAN (802.1Q): Przypisanie dedykowanych adresów IP i tagów VLAN dla interfejsów logicznych: Management, Storage (VMware) oraz Backup (Klienci).
- ☐ Fortigate UTM (L3/L4): Wdrożenie polityk ACL dla serwera i agentów. Konfiguracja szyfrowanego dostępu administracyjnego via VPN (z zewnątrz), Zamawiający posiada aktualne licencje.
- ☐ Wydzielenie zasobów i izolacja sieci - Wykonawca dokona fizycznej i logicznej separacji interfejsów sieciowych serwera, podłączając urządzenie niezależnie do infrastruktury sieci produkcyjnej oraz odseparowanej sieci monitoringu. W ramach architektury pamięci masowej wymagane jest wydzielenie 20TB na dane materiału wideo, oraz konfigurację w wydzielonej przestrzeni poprzez iSCSI w systemie wizyjnym (szczegółowe dane systemu monitoringu oraz jego dokumentacja do wglądu u Zamawiającego)

Faza 3: Warstwa składowania i wirtualizacji

- ☐ Konfiguracja macierzy RAID: Inicjalizacja wolumenów w bezpiecznej architekturze (RAID 6 lub RAID F1) zapewniającej ochronę przed jednoczesną awarią dwóch nośników.

- ☐ Szyfrowanie i Bezpieczeństwo Danych: Aktywacja sprzętowego mechanizmu szyfrowania danych (AES-256) na poziomie wolumenów. Konfiguracja protokołów SMB/NFS z uwierzytelnianiem Kerberos oraz integracją z listami kontroli dostępu (ACL).
- ☐ Integracja VMware ESXi, Konfiguracja kopii zapasowych środowiska VMware przy użyciu zaawansowanego oprogramowania klasy Enterprise (np. Veeam lub równoważnego, natywnego oprogramowania dostarczonego w ramach licencji producenta serwera NAS), zapewniająca utrzymanie co najmniej 3 pełnych kopii oraz obowiązkową kopię typu offline. Kopia offline raz w tygodniu w każdy poniedziałek (Auto-unmount), należy zapewnić dodatkowy nośnik 20TB kompatybilny z dostarczonym urządzeniem NAS (połączenie poprzez USB).
- ☐ Integracja AD: Dołączenie do domeny. Mapowanie uprawnień NTFS/Windows ACL dla zasobów plikowych.

Faza 4: Implementacja Systemu Zarządzania i Monitorowania IT

- ☐ Konfiguracja maszyny wirtualnej w klastrze vSphere
- ☐ Konfiguracja systemu backupu
- ☐ Wdrożenie rdzenia systemu (SNMP): Uruchomienie platformy klasy Enterprise monitorującej infrastrukturę poprzez protokół SNMP v3. Konfiguracja automatycznego wykrywania nowych urządzeń w sieci.
- ☐ Dystrybucja Agentów: Instalacja komponentów klienckich na 80 stacjach roboczych i 10 serwerach (nie wszystkie komputery w AD). Agent musi pracować jako usługa systemowa w trybie stealth.
- ☐ Konfiguracja modułów DLP i Szyfrowania: * Wdrożenie polityk Data Loss Prevention (blokowanie portów USB, audyt operacji na plikach).
 - Centralne zarządzanie szyfrowaniem BitLocker z bezpiecznym składowaniem kluczy odzyskiwania w konsoli administratora.
- ☐ Audyt i Inwentaryzacja: Automatyczne pobranie danych o sprzęcie i oprogramowaniu, w tym ewidencja numerów seryjnych, terminów gwarancji oraz skanów licencji i faktur.
- ☐ Zdefiniowanie harmonogramów automatycznej i cichej instalacji brakujących poprawek systemowych dla środowiska Windows, bez przerywania pracy użytkowników.
- ☐ Zdefiniowanie uprawnień w konsoli webowej dla administratorów i kierowników (dostęp tylko do wybranych dashboardów i logów).
- ☐ Pozostała konfiguracja zgodna z wytycznymi dokumentu „Minimalne Wymagania IT COS OPO Cetniewo” do wglądu u Zamawiającego (szacunkowy dodatkowy czas pracy specjalisty IT do 30 godzin)
- ☐ Przeprowadzenie szkolenia z funkcjonalności oprogramowania

Faza 5: Backup, Dokumentacja i Testy

- ☐ Polityka 3-2-1 i Offline Backup: Konfiguracja zadań backupu (np. Veeam) z macierzy Alcatel na serwer NAS. Wykonawca musi zapewnić kopię typu "offline" (niezależną od uprawnień domeny), chroniącą przed atakami ransomware, Wykonawca musi zapewnić nośnik do kopii offline.
- ☐ Dokumentacja Powykonawcza: Dostarczenie kompletnego kompendium: topologii logicznej, tablicy adresacji IP, rejestru ryzyk oraz szczegółowych procedur awaryjnych.

- ☐ Testy Akceptacyjne: Udokumentowane testy przełączania awaryjnego, odtwarzania danych z kopii oraz symulacja zaniku zasilania.

5. Wymagania gwarancyjne oraz reżim świadczenia usług serwisowych (SLA) dla systemu NAS i oprogramowania IT:

Poniższe warunki stanowią krytyczny element realizacji zamówienia. Wymaga się od Wykonawcy gotowości do świadczenia zaawansowanego wsparcia technicznego o parametrach klasy Enterprise dla dostarczonych komponentów, przy bezwzględnym zachowaniu procedur bezpieczeństwa środowiska informatycznego.

1. Precyzyjny zakres i czas trwania gwarancji

- ☐ Przedmiot gwarancji: Wykonawca udziela pełnej gwarancji wyłącznie na fabrycznie nowe elementy dostarczone w ramach postępowania, tj.:
 1. Serwer NAS
 2. 12 fizycznych dysków twardych o pojemności min. 12 TB każdy, wykonanych w technologii CMR, pochodzących od tego samego producenta co serwer.
 3. Oprogramowanie do zarządzania i monitorowania IT (klasy Enterprise) wraz z licencjami na min. 80 klientów.
- ☐ Wyłączenia sprzętowe: Gwarancja nie obejmuje istniejącej infrastruktury (Fortigate 100F, przełączniki Cisco/Alcatel, macierz Alcatel). Wykonawca gwarantuje jednak pełną kompatybilność i stabilną współpracę dostarczonego środowiska z wymienionymi urządzeniami.
- ☐ Okres gwarancyjny: Na dostarczony serwer, oprogramowanie oraz dyski twarde Wykonawca udziela bezwzględnej gwarancji na okres min 36 miesięcy (3 lat) od daty podpisania bezusterkowego protokołu odbioru końcowego.

2. Rygorystyczne warunki SLA (Service Level Agreement)

Wykonawca musi zapewnić stałą gotowość do natychmiastowego podjęcia działań naprawczych w przypadku awarii sprzętowej lub błędów oprogramowania.

- ☐ Czas przystąpienia do usunięcia awarii na miejscu (On-site Response Time): W przypadku awarii krytycznej (np. usterka dysku degradująca macierz, błąd systemu monitorowania uniemożliwiający nadzór), Wykonawca jest zobowiązany do podjęcia prac przez autoryzowanego inżyniera bezpośrednio w lokalizacji Zamawiającego w czasie nie dłuższym niż 12 godzin od zgłoszenia.
- ☐ Czas przywrócenia funkcjonalności (Resolution Time): Awaria musi zostać usunięta, a pełna funkcjonalność systemu przywrócona najpóźniej w ciągu 48 godzin. Dla oprogramowania oznacza to przywrócenie usług z kopii zapasowej (offline); dla serwera NAS – fizyczną naprawę lub dostarczenie sprzętu zastępczego.
- ☐ Zarządzanie zmianą: Każda zmiana rekonfiguracyjna w systemie musi być nadzorowana i dokumentowana w dzienniku systemu.

3. Procedura obsługi awarii dysków twardych ("Keep Your Drive")

Z uwagi na fakt, że obszar sieci serwerowej jest przestrzenią przetwarzania danych osobowych, obowiązuje rygorystyczna procedura wymiany nośników:

- ☐ Zatrzymanie nośnika: Wszystkie uszkodzone lub wymieniane dyski twarde, na których pracowały systemy Ośrodka, bezwzględnie pozostają własnością Zamawiającego.
- ☐ Fizyczna utylizacja: Nośniki podlegają udokumentowanej utylizacji przeprowadzanej przez Zamawiającego. Wykonawca musi uwzględnić brak zwrotu uszkodzonego nośnika w procesie RMA w wycenie oferty.

4. Wymogi bezpieczeństwa podczas interwencji

Każda interwencja inżyniera podlega surowym procedurom kontrolnym:

- ❓ Dostęp zdalny: Możliwy wyłącznie za pośrednictwem tunelu szyfrowanego VPN-SSL (wyłącznie sprzęt służbowy) po każdorazowej decyzji Dyrektora lokalizacji. Wszystkie dostępy muszą być ewidencjonowane i uzasadnione.
- ❓ Protokołowany dostęp do poświadczeń: Użycie haseł administracyjnych przechowywanych w tzw. "bezpiecznych kopertach" wymaga sporządzenia protokołu (kto, kiedy, dlaczego).
- ❓ Rotacja poświadczeń: Po zakończeniu prac, każde użyte hasło musi zostać niezwłocznie zmienione w celu zachowania pełnej rozliczalności i ponownie zdeponowane w bezpiecznej kopercie.

5. Gwarantowane wsparcie konfiguracyjne

- ❓ Rozwój i rekonfiguracja: W ramach wykupionej usługi asysty technicznej (SLA), Wykonawca jest zobowiązany do świadczenia wsparcia inżynierskiego polegającego na wdrażaniu dodatkowych konfiguracji, modyfikacji istniejących ustawień Systemie Zarządzania i Monitorowania IT na wyraźne żądanie Zamawiającego, zgłoszone prze
- ❓ Okno serwisowe i czas reakcji: Usługa realizowana jest w dni robocze (od poniedziałku do piątku) w godzinach 8:00 – 16:00. Czas pełnej realizacji zgłoszenia – rozumiany jako ostateczne wdrożenie, przetestowanie i oddanie nowej konfiguracji przez inżyniera – nie może przekroczyć **48 godzin** od momentu zarejestrowania oficjalnego wniosku przez autoryzowanego pracownika Zamawiającego.