Załącznik nr 6 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Komputer biurkowy - 15 szt**

Komputer stacjonarny. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego. Nie dopuszcza się zaoferowania komputera refurbished. Zamawiający nie dopuszcza żadnej ingerencji w sprzęt, rozbudowy lub modyfikacji. Konfiguracja fabryczna producenta komputera.				Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**	
1	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej.		
2	Obudowa	Typu SFF z obsługą kart PCI Express o niskim profilu: - 1 x PCI Express x16, - 1 x PCI Express x1, Wyposażona w min: - 1 szt. 5,25” (dopuszcza się zastosowanie jednej kieszeni 5,25” w wersji SLIM dla napędu optycznego) - 1 szt. 3,5” + 1 szt. 2,5’’ lub 2 szt. 2,5” Obudowa musi być wyposażona w czujnik otwarcia. Wbudowany głośnik o mocy 1W Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnym		
3	Chipset	Dostosowany do zaoferowanego procesora		
4	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 2 złącza M.2 z czego 1 dedykowane dla dysku SSD PCIe.		
5	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach min. 16 300 pkt. w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/.		

		Testy pochodzące z okresu od publikacji postępowania do dnia składania ofert. Wydruk z wynikami testów należy załączyć do oferty.	
6	Pamięć operacyjna	8GB, 3200MHz DDR4, 4 sloty na pamięć, z czego min. 3wolne. Możliwość rozbudowy pamięci do 128GB RAM.	
7	Dysk twardy	Min 256GB M.2 PCIe, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
8	Napęd optyczny	Nagrywarka DVD +/-RW	
9	Karta graficzna	Zintegrowana karta graficzna z procesorem.	
10	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
11	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 wspierająca WoL	
12	Porty/złącza	Wbudowane porty: - 1 x HDMI, - 2 x DP, - 1 x USB 3.2 Typ-A, 4x USB 3.2, 2x USB 3.0 Typ-A z przodu obudowy - 1 x USB-C z przodu obudowy - port sieciowy RJ-45, - port szeregowy RS-232 - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy - czytnik kart pamięci Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
13	Klawiatura/mysz	Klawiatura w układzie US + mysz optyczna z rolką	
14	Zasilacz	Energooszczędny zasilacz o mocy 240W oraz sprawności na poziomie min. 85%.	
15	System operacyjny	Microsoft Windows 11 Professional PL w wersji komercyjnej / OEM lub równoważny. System zainstalowany przez producenta komputera. Klucz licencji systemu operacyjnego wpisany w pamięć BIOS komputera. Zamawiający nie dopuszcza wersji edukacyjnych / refurbished / STF / Acdmc.	

		Zamawiający dopuszcza rozwiązanie równoważne: System zainstalowany przez producenta komputera. Nie wymagający aktywacji za pomocą Internetu lub telefonu. Zainstalowany system operacyjny, w polskiej wersji językowej. Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu. System operacyjny klasy desktop, 64-bit. Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym: 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy; 2) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym: 1) polskim; 2) angielskim. Zlokalizowane w języku polskim, co najmniej następujące elementy: 1) menu; 2) odtwarzacz multimediów; 3) pomoc; 4) komunikaty systemowe. Wbudowany system pomocy w języku polskim. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.	

		Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. Zintegrowana z systemem operacyjnym konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie.	

		Możliwość pracy systemu w trybie ochrony kont użytkowników. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa /instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, w tym: 1) poziom menu; 2) poziom otwartego okna systemu operacyjnego. Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Obsługa standardu NFC (near field communication). Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. Mechanizmy logowania do domeny w oparciu o: 1) login i hasło; 2) karty z certyfikatami (smartcard); 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). Mechanizmy wieloelementowego uwierzytelniania. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. Wsparcie dla algorytmów Suite B (RFC 4869). Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.	

		Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. Udostępnianie modemu. Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa	

		(z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinsatalacji systemu. Obsługa pracy domenowej w środowisku Active Directory dla systemów Microsoft Windows Server.	
16	BIOS	Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera - numerze seryjnym, - numerze inwentarzowym (tzw. Asset Tag),	

		- MAC Adres karty sieciowej, - wersja Biosu, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji bootujących (podstawowa, po awarii) - załadowania optymalnych ustawień Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.	
17	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test magistrali PCI-e • test portów USB • test płyty głównej	

		Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja • Procesor: Nazwa, taktowanie • Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	
18	Certyfikaty i standardy	• Certyfikat ISO 9001 dla producenta sprzętu • Certyfikat ISO 50001 dla producenta sprzętu • Energy Star min. 8.0 • Certyfikat TCO • Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	
19	Waga/rozmiary urządzenia	Suma wymiarów obudowy nie może przekraczać 735 mm.	
20	Bezpieczeństwo	Złącze typu Kensington Lock Moduł TPM 2.0 z certyfikacją TCG	
21	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.	
22	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji	

		bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.	
23	Gwarancja	36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site) Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	
24	Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
25	Monitor	Rozmiar matrycy minimum 23,8” Typ matrycy: IPS Powierzchnia matrycy: Antyodblaskowa, utwardzona Rozdzielczość natywna minimum 1920x1080 FHD Kontrast statyczny minimum 1 000:1 Kontrast dynamiczny minimum 100 000 000:1 Proporcje: 16:9 Jasność minimum 250 cd/m2 Odświeżanie matrycy minimum 60 Hz Czas reakcji nie więcej niż 4ms Monitor wyposażony w tzw. Kensington Slot Zakres regulacje: Regulacja kąta pochylenia, Regulacja wysokości, Obrót SWIVEL, Możliwość obrotu o 90 stopni ekranu na podstawie (PIVOT) Głośniki: wbudowane, min. 2x 1,5W Poziomy/pionowy kąt widzenia: 178/178 stopni Porty minimum: 1x VGA; 1x HDMI, 1x Displayport Wyposażenie w zestawie: kabel HDMI, kabel zasilający, kabel VGA, kabel audio	

		Gwarancja producenta na okres minimum 36 miesięcy	

2. Serwery wraz z oprogramowaniem – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)	
Typ	Minimalne wymagania	Oferowane rozwiązanie
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.	
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.8GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	
RAM	Minimum 128GB DDR4 RDIMM 3200MT/s , na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing	
Gniazda PCI	- minimum dwa sloty PCIe x16 generacji 4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+(OCP 3.0) (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD	

	Zainstalowane 6 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.	
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.	
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.	
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200	
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.	
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem	
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej;	

	• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów, Microsoft Windows 2016, Microsoft Windows 2019.	
Warunki gwarancji	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany	

	bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
System operacyjny	Do każdego serwera należy dostarczyć oprogramowanie Windows Server 2022 Standard z możliwością uruchomienia 6 maszyn wirtualnych oraz 12 licencji dostępowych na użytkownika lub równoważny.	

3. Oprogramowanie do wirtualizacji

	Minimalne wymagania	Oferowane rozwiązanie
Specyfika oprogramowania	Wirtualizacja z centralnym zarządzeniem	
Serwer zarządzający	Nazwa oprogramowania	
Maks. ilość hostów ESXi	Min. 3	
Maks. ilość CPU/Host	Min. 2	
Maks. ilość VM/Host	Min. 1024	
Typ licencji	Licencja wieczysta z prawem do aktualizacji na podstawie aktualnej subskrypcji	
	Funkcjonalności	
vSphere Hypervisor	TAK	
vCenter Server Essentials	TAK	
vSphere VMFS	TAK	
VMware vSphere vStorage APIs	TAK	
Licencja	Min. 3 lata	

4. Oprogramowanie do pracy zdalnej ZOOM z subskrypcją na 3 lata

L.p	Minimalne wymagania	
Oprogramowanie do prowadzenia wideokonferencji – 3 letnia licencja		
1	Maksymalna liczba uczestników min. 100	
2	Liczba licencji - 1	
3	Nielimitowana ilość spotkań	
4	Maksymalny czas trwania spotkania grupowego min. 30h	
5	Nagrywanie lokalne + chmurowe(min. 1GB/licencję)	
6	Udostępnianie ekranu	
7	Breakout rooms (podział na pokoje)	
8	Wirtualne tło	
9	Osobisty ID spotkania	
10	Prywatny i grupowy czat	
11	Funkcja hosta	
12	Adnotacje	
13	Przekazanie kontroli	
14	Biała tablica	
15	Udostępnianie kilku ekranów jednocześnie	
16	Szyfrowanie TLS	
17	Szyfrowanie AES256	
18	Poczekalnia	
19	Przypnij wiele osób	
20	Wyróżnij wiele osób	
21	Filtry	
22	Ankiety	
23	Co-host i alternatywny host	
24	Planowanie i harmonogram spotkań	
25	Streaming	
26	Raporty	
27	Zarządzanie użytkownikami	
28	Transkrypcja na żywo	
29	Portal Admina	
30	Integracja LTI	
31	Nagrywanie transkrypcji	
32	Branding	
33	Zarządzanie domenami	
34	SSO	
35	Tłumaczenie symultaniczne	

5. Oprogramowanie do skanowania podatności zagrożeń w sieci lokalnej

Wymagane parametry	
Oprogramowanie zapewniające badanie podatności sieci na ataki	Producent: Nazwa oprogramowania:
1. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym.	
2. Architektura rozwiązania składać się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania.	
3. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej.	
4. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta lub w postaci oprogramowania instalowanego w lokalnej infrastrukturze informatycznej.	
5. Rozwiązanie posiada opcję przechowywania wszystkich danych o wykrytych podatnościach w lokalnej sieci zamawiającego.	
6. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych:	
• Microsoft Edge	
• Mozilla Firefox	
• Google Chrome	
• Safari	
7. Centralna konsola zarządzania, instalowana lokalnie w infrastrukturze zamawiającego, oferuje możliwość instalacji na systemie Windows Server 2012 R2 i nowszych	
8. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania.	
9. Oprogramowanie skanujące podatności jest również dostępne w postaci usługi hostowanej na serwerach producenta oprogramowania.	
10. Oprogramowanie skanujące podatności w formie usługi jest zarządzane za pomocą tej samej konsoli zarządzania co oprogramowanie skanujące zainstalowane lokalnie.	

11. Oprogramowanie skanujące podatności, w postaci aplikacji instalowanej lokalnie, wspiera poniższe systemy operacyjne:	
• Windows Server 2012 R2 i nowsze	
• Ubuntu server 18.x LTS	
12. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.	
13. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:	
a) wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP.	
b) wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych.	
c) Pozwala na konfigurację parametrów skanowania takich jak:	
a. zakres przeszukiwanych portów,	
b. wydajność skanowania (ilość jednoczesnych połączeń sieciowych),	
c. liczbę jednoczesnych wątków skanowania,	
d. możliwość wykrycia wersji systemu operacyjnego.	
d) konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania)	
e) konfigurację wysyłania powiadomień na wskazany adres e-mail, informujących o rozpoczęciu skanowania oraz jego zakończeniu.	
14. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.	
15. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLS oraz XML.	
16. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.	
17. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:	

a) określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP.	
b) masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV.	
c) konfigurację parametrów skanowania, takich jak:	
a. zakres skanowanych portów sieciowych TCP/UDP,	
b. parametr wydajności skanowania,	
c. rodzaj uwierzytelniania na skanowanej stacji.	
d) konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia.	
e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.	
18. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.	
19. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku XLS oraz XML.	
20. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.	
21. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:	
a) określenie skanowanego celu za pomocą adresu URL lub adresu IP.	
b) konfigurację parametrów skanowania takich jak:	
a. rodzaje testowanych ataków,	
b. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web),	
c. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).	
c) konfigurację uwierzytelniania w testowanej aplikacji web.	

d) konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania.	
e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.	
22. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.	
23. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.	
24. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:	
a) przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania.	
b) zapisywanie wskazanych warunków wyszukiwania jako szablony.	
c) podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych.	
d) dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.	
25. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.	
26. Lista wszystkich wykrytych podatności musi umożliwiać:	
a) filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (opis), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy.	
b) wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta.	

c) eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.	
27. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów.	
28. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego.	
29. Raport podsumowujący umożliwia:	
a) konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu,	
b) wybranie grup urządzeń, które będą znajdowały się w raporcie,	
c) wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie,	
d) personalizację danych, którymi zostanie podpisany raport.	
30. Lista wygenerowanych raportów musi umożliwiać:	
a) filtrowanie raportów ze względu na ich autora, nazwę, szablon oraz opis,	
b) eksport wyniku raportu do pliku XML, DOCX, XLS.	
31. Rozwiązanie umożliwia zarządzanie wykrytymi podatności w co najmniej następujący sposób:	
a) podgląd listy utworzonych zgłoszeń,	
b) filtrowanie zgłoszeń ze względu na ich status oraz czas zamknięcia,	
c) podgląd listy szablonów dla poszczególnych rodzajów skanów,	
d) dodanie szablonu dla poszczególnych rodzajów skanów oraz wprowadzenie ich konfiguracji,	
e) zarządzanie listą użytkowników oraz przypisywanie ich do grupy,	
f) konfigurację grup użytkowników z odpowiednimi uprawnieniami do poszczególnych grup skanów,	
g) wprowadzenie restrykcji adresu IP z którego następuje logowanie,	
h) wymuszenie weryfikacji dwuetapowej podczas logowania,	
i) podgląd wszystkich zdarzeń w systemie uwzględniając użytkownika, adres IP oraz rodzaj zdarzenia,	
j) wykorzystanie API do integracji danych z innymi środowiskami.	
32. Liczba licencji - 24	