Załącznik nr 1 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ 1

„Utworzenie środowiska zapewniającego ciągłość działania systemów informatycznych Urzędu Miejskiego w Pabianicach”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest utworzenie środowiska zapewniającego ciągłość działania systemów informatycznych Urzędu Miejskiego w Pabianicach, w szczególności poprzez dostawę klastra niezawodnościowego wysokiej dostępności składającego się z: dwóch macierzy dyskowych wraz z niezbędnymi licencjami, czterech przełączników Fibre-Channel, trzech kart Fibre-Channel do istniejących serwerów oraz Serwera quorum z kartą Fibre Channel wraz z wdrożeniem

Przedmiot zamówienia obejmuje zakup urządzeń o opisanej niżej konfiguracji sprzętowej wraz z dostawą do siedziby zamawiającego, montażem oraz wstępną konfiguracją, a także usługami konfiguracji, szkoleniem i trzyletnim wsparciem.

Ilekroć niżej mowa o oprogramowaniu urządzeń lub ich cechach, właściwościach i funkcjach, zakłada się, że ewentualne związane z nimi licencje będą dostarczone wraz ze sprzętem, w cenie urządzeń, chyba że wyraźnie zastrzeżono inaczej.

Celem zamówienia jest przebudowa istniejącego środowiska w kierunku dwuośrodkowego klastra active-active opartego o trzy niezależne ośrodki z funkcjonalnością autonomicznego przełączania usług w przypadku utraty dowolnego ośrodka. Skuteczne zarządzanie infrastrukturą Urzędu musi przewidywać również odpowiednie mechanizmy ochrony danych przed ich utratą, nie tylko będącą efektem awarii, czy katastrof, ale również celowego działania niszczycielskiego typu atak ransomware. W ramach zamówienia, obecnie stosowane zabezpieczenia należy przebudować korzystając z nowoczesnych rozwiązań oferowanych przez dostarczane macierze dyskowe, w połączeniu z posiadanym oprogramowaniem backupowym Veeam.

System musi przewidywać procedury replikacji danych wewnątrz ośrodkowych i między ośrodkowych, które zabezpieczą go przed cyber-atakami.

Wykonawca przed podpisaniem umowy ma obowiązek przedłożyć Zamawiającemu dokumenty, z których bezspornie wynika, że objęte ofertą produkty są zarejestrowane w systemie gwarancyjnym producenta i uprawniają Zamawiającego do korzystania w pełni z przysługujących mu w tym zakresie praw gwarancyjnych.

2. Opis techniczny oferowanych urządzeń

Przedmiotem zamówienia jest zakup, dostawa i wdrożenie niżej opisanego sprzętu.

Serwer wirtualizacyjny usługi metroklastra – 1 sztuka	
Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia); Serwer wyposażony w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków; Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą; Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie, aplikacja zarządzająca dostępna na Android i iOS.
Procesor	Dwa procesory dwunastordzeniowe, x86 - 64 bity, osiągające w testach PassMark (https://www.cpubenchmark.net) wynik nie gorszy niż 41150 punktów w konfiguracji dwuprocesorowej, posiadające zestaw instrukcji wspierający wirtualizację
Płyta główna	Płyta główna wspierająca zastosowanie procesorów 32 rdzeniowych, posiadająca minimum 16 gniazd pamięci i umożliwiająca obsługę minimum 1TB pamięci operacyjnej
Pamięć operacyjna	192 GB RDIMM DDR4 3200MT/s w modułach o pojemności min. 16GB każdy.
Sloty rozszerzeń	3 aktywne gniazda PCI-Express generacji 4, w tym min. 1 slot x16 (szybkość slotu – bus width)
Pamięć masowa	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” Zainstalowane dwa dyski SSD 2,5” typu MixedUse o pojemności min. 480GB każdy. Możliwość instalacji pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 64GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.
Kontroler	Serwer wyposażony w kontroler sprzętowy zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10.

Interfejsy sieciowe	Minimum 2 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń"; Minimum 2 porty FC 16Gb wraz z wkładkami; Minimum 2 porty SFP 10Gb wraz z wkładkami; Opcja rozbudowy o dodatkowe 2 porty obsługujące prędkości 10/25 Gb/s (możliwość konfiguracji pracy z prędkościami 10 i 25Gb/s), przez zastosowanie karty nie zajmującej gniazd PCIe opisanych w sekcji „Sloty rozszerzeń".
Karta graficzna	Zintegrowana karta graficzna.
Porty	1 x USB 3.0 z przodu serwera; 1 x USB 3.0 wewnątrz serwera; 2 x USB z tyłu serwera, w tym min. jeden port 3.0; 1 x VGA z przodu serwera; 1 x VGA z tyłu serwera; Możliwość wyposażenia w port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug.
Napęd	Możliwość instalacji napędu DVD-ROM lub DVD-RW w obudowie serwera
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • 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 SNMP; IPMI2.0, VLAN tagging, SSH; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.; • możliwość zdalnego ustawienia limitu poboru prądu przez serwer; • integracja z Active Directory;

	• możliwość obsługi przez ośmiu administratorów jednocześnie; • wsparcie dla automatycznej rejestracji DNS; • wsparcie dla LLDP; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; • możliwość podłączenia lokalnego poprzez złącze RS-232; • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy; • monitorowanie zużycia dysków SSD; • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi; • automatyczne zgłaszanie alertów do centrum serwisowego producenta; • automatyczne update firmware dla wszystkich komponentów serwera; • możliwość przywrócenia poprzednich wersji firmware; • możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON; • możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych; automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware ESXi, Citrix Hypervisor, Canonical Ubuntu Serwer LTS.
Wsparcie techniczne	Minimum 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Producent musi umożliwiać rozszerzenie gwarancji do 7 lat. Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka. Powinna być dostępna możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. messenger, teams, WhatsApp.

	Firma serwisująca musi posiadać certyfikat ISO 9001 na świadczenie usług serwisowych lub normą równoważną spełniającą wszystkie wymagania tej normy oraz posiadać autoryzacje producenta urządzeń. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Prawo zachowania dysku (KYHD)	Prawo zachowania dysku u Zamawiającego w przypadku jego awarii
Inne	Urządzenia muszą być fabrycznie nowe i nieużywane. Wykonawca przed podpisaniem umowy musi przedstawić dokumenty potwierdzające, że oferowany serwer, pochodzi z oficjalnego kanału dystrybucyjnego producenta i że produkt ten jest zarejestrowany w systemie gwarancyjnym producenta a uprawnionym do roszczeń gwarancyjnych jest Miasto Pabianice. Wymagane są dokumenty: • certyfikat poświadczający, że sprzęt jest produkowany zgodnie z normą ISO 9001 lub normą równoważną spełniającą wszystkie wymagania ww. certyfikatu, • certyfikat poświadczający, że sprzęt jest produkowany zgodnie z normą ISO 14001 lub normą równoważną spełniającą wszystkie wymagania ww. certyfikatu, • deklaracja zgodności CE.

Macierze dyskowe usługi metroklastra – 2 sztuki	
Obudowa	Obudowa o wysokości maksymalnie 3U dedykowana do zamontowania w szafie rack 19 cali z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Co najmniej 24 zatoki przystosowane do instalacji dysków SSD NVMe.
Kontroler dyskowy	Zainstalowane minimum dwa redundantne kontrolery pamięci dyskowej, pracujące w trybie symetrycznym Active-Active, obsługujące protokół komunikacji NVMe z dyskami. Pod określeniem tryb Active-Active Zamawiający rozumie, że zasób pamięci dyskowej jest równolegle dostępny na co najmniej 8 portach należących do co najmniej 2 różnych kontrolerów pamięci dyskowej. Każdy z kontrolerów musi mieć możliwość prezentacji

	wszystkich wolumenów utworzonych w ramach całej pamięci dyskowej.
Zasilacz	Dwa w pełni redundantne zasilane prądem 230 V.
Porty sieciowe FC	Każdy z dostarczanych kontrolerów pamięci dyskowej musi być wyposażony w co najmniej 4 interfejsy FC, każdy o przepustowości co najmniej 32 Gbps. Każdy z zainstalowanych interfejsów FC musi być obsadzony wkładką FC Short Range Multi Mode SFP+ o przepustowości co najmniej 16Gbps.
Porty sieciowe iSCSI	Każdy z dostarczanych kontrolerów pamięci dyskowej musi być wyposażony w co najmniej 2 interfejsy iSCSI, każdy o przepustowości co najmniej 10 Gbps. Każdy z zainstalowanych interfejsów iSCSI musi być obsadzony wkładką optyczną SFP+ o przepustowości co najmniej 10Gbps.
Dyski	Co najmniej 8 wewnętrznych dysków SSD, każdy w technologii co najmniej NVMe 1.4, każdy o pojemności co najmniej 3.8 TB i posiadający podwójne interfejsy do komunikacji z kontrolerami pamięci dyskowej.
Gwarancja	Co najmniej 36 miesięcy od daty dostawy. Gwarancja świadczona w miejscu instalacji sprzętu, z czasem naprawy w kolejnym dniu roboczym od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej. Gwarancja realizowana przez producenta lub jego autoryzowanego partnera serwisowego.
Inne	Urządzenia muszą być fabrycznie nowe i nieużywane. Wykonawca przed podpisaniem umowy musi przedstawić dokumenty potwierdzające, że oferowany serwer, pochodzi z oficjalnego kanału dystrybucyjnego producenta i że produkt ten jest zarejestrowany w systemie gwarancyjnym producenta a uprawnionym do roszczeń gwarancyjnych jest Miasto Pabianice. Wymagane są dokumenty: • certyfikat poświadczający, że sprzęt jest produkowany zgodnie z normą ISO 9001 lub normą równoważną spełniającą wszystkie założenia ww. certyfikatu, • certyfikat poświadczający, że sprzęt jest produkowany zgodnie z normą ISO 14001 lub normą równoważną spełniającą wszystkie założenia ww. certyfikatu, • deklaracja zgodności CE.

Parametry szczegółowe

1. Pełna wewnętrzna redundancja kontrolerów, portów wewnętrznych, zasilania, chłodzenia i ścieżek danych na poziomie minimum N+1.
2. Możliwość uaktualniania oprogramowania systemowego bez przerywania działania pamięci dyskowej z utrzymaniem wszystkich funkcjonalności.

3. Pamięć dyskowa musi być wyposażona w system zapewniający bezpieczne, bez utraty danych, automatyczne wyłączenie w przypadku całkowitego zaniku zasilania,
4. Pamięć dyskowa musi umożliwiać wymianę kontrolerów, zasilaczy i wentylatorów w trybie Hot Swap - w trakcie pracy pamięci dyskowej.
5. Pamięć dyskowa musi umożliwiać stosowania dysków Hot Spare i wymianę dysków w trybie Hot Swap.
6. Pamięć dyskowa musi posiadać zainstalowaną pamięć cache o pojemności fizycznej co najmniej 384 GB. Nie dopuszcza się użycia pamięci cache zbudowanej w formie dysków SSD lub Flash itp.
7. W przypadku awarii zasilania niezsynchronizowane dane w pamięci cache muszą być zabezpieczone metodą trwałego zapisu do pamięci nieulotnej lub pamięć powinna być podtrzymana bateryjnie przez minimum 72h.
8. Pamięć dyskowa musi obsługiwać standard NVMe w wersji co najmniej 1.4.
9. Pamięć dyskowa musi umożliwiać instalację dysków wewnętrznych w standardzie minimum NVMe i SAS-3.
10. Pamięć dyskowa musi umożliwiać instalację następujących interfejsów sieciowych:
    10.1. Co najmniej 24 interfejsów FC, każdy o przepustowości co najmniej 32 Gbps.
    10.2. Co najmniej 12 interfejsów iSCSI, każdy o przepustowości co najmniej 10Gbps.
11. Oferowane funkcjonalności i parametry muszą być możliwe do zweryfikowania na ogólnie dostępnej stronie internetowej producenta w celu sprawdzenia, że oferowany produkt spełnia ww. wymagania.
12. Dostarczone oprogramowanie i funkcjonalności muszą być udostępniane przez firmware bez modyfikacji przez Wykonawcę i jest to standardowe oprogramowanie producenta. Zamawiający nie dopuszcza takiej sytuacji, w której oprogramowanie pamięci dyskowej jest specjalnie przygotowane dla Zamawiającego.
13. Pamięć dyskowa musi posiadać wbudowane, realizowane przez kontrolery, mechanizmy kompresji i deduplikacji danych w trybie in-line.
14. Pamięć dyskowa musi oferować wsparcie dla funkcjonalności zdalnej replikacji danych w trybie synchronicznym i asynchronicznym za pomocą sieci SAN oraz replikację typu Metro Cluster (równoległy dostęp do obu wolumenów w każdej parze replikacyjnej w trybie zapisu i odczytu). Oprogramowanie musi zapewniać funkcjonalność zawieszania replikacji i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zmiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora.
15. Pamięć dyskowa musi oferować wsparcie dla architektury dwuośrodkowej DR wykorzystującej do zarządzania oprogramowanie VMware SRM.
16. Pamięć dyskowa musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point in time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Oferowane urządzenie musi obsługiwać minimum 500 000 kopii migawkowych (1024 per udział/dysk logiczny). Realizacja kopii migawkowych w trybie Copy-on-Write nie jest dopuszczona.

17. Oprogramowanie pamięci dyskowej musi umożliwiać automatyczne, na podstawie zdefiniowanych polityk dostosowanych do wymagań RPO chronionych zasobów, tworzenie i usuwanie kopii migawkowych i klonów.
18. Pamięć dyskowa musi umożliwiać blokowanie czasowe kopii migawkowych i klonów bez możliwości usunięcia blokady i chronionych kopii przed upływem określonego terminu retencji czy to przez administratora macierzy czy inżyniera producenta.
19. Pamięć dyskowa musi umożliwiać tworzenie kopii migawkowych i klonów z zasobów chronionych usługą klastra active-active macierzy.
20. Pamięć dyskowa musi umożliwiać integrację z oprogramowaniem backupowym Veeam Backup & Replication na poziomie umożliwiającym pełną współpracę w zakresie:
    20.1. backupu z migawek pamięci masowych,
    20.2. Veeam Explorer for Storage Snapshots,
    20.3. On-Demand Sandbox for Storage Snapshots
21. Pamięć dyskowa musi umożliwiać migrację dysków logicznych pomiędzy grupami zabezpieczonymi różnymi typami RAID. Migracja odbywa się w trybie on-line bez przerywania pracy systemu/aplikacji korzystającej z danych migrowanego woluminu.
22. Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS dla wybranych wolumenów logicznych w zakresie: wydajności w IOPS, wydajność w MB/s.
23. Pamięć dyskowa musi umożliwiać wirtualizację posiadanych przez Zamawiającego zasobów dyskowych Jako wirtualizacje definiuje się zabieg techniczny polegający na udostępnieniu wirtualizowanych zasobów dyskowych klientom wirtualizatora z możliwością wykorzystania dodatkowych funkcjonalności specyficznych dla tego wirtualizatora, a nie posiadanych przez urządzenie wirtualizowane. Mechanizm wirtualizacji musi być wbudowany w oprogramowanie wewnętrzne oferowanej pamięci dyskowej i nie może być realizowany z wykorzystaniem dodatkowych zewnętrznych urządzeń i oprogramowania.
24. Wirtualizacja zasobów wewnętrznych musi umożliwiać utworzenie przynajmniej 2 wirtualnych macierzy dla przynajmniej 2 hostów, z możliwością delegowania przestrzeni, portu, przepustowości i spodziewanej wydajności. Parametry tych wirtualnych macierzy określamy poprzez ustalenie QOS dla danej usługi Hosta.
25. Nie jest dopuszczalne rozwiązanie, w którym usługi protokołu Fibre Channel realizowane są w oparciu o emulację protokołu FC na wewnętrznym systemie plików pamięci dyskowej.
26. Jeśli jest to konieczne, wraz z pamięcią dyskową muszą zostać dostarczone licencje na funkcję kontrolerów umożliwiającą wykorzystywanie obu kontrolerów pamięci dyskowej w taki sposób, aby oprogramowanie zainstalowane w systemie operacyjnym klienta (serwera do wirtualizacji pamięci dyskowej) automatyczne przełączało ścieżki do zasobów, np. w przypadku uszkodzenia portu karty HBA, przełącznika SAN, kontrolera pamięci dyskowej czy przewodu światłowodowego.
27. Dostarczane oprogramowanie zarządzające pamięcią dyskową oraz licencje umożliwiają:
    27.1. stałe monitorowanie stanu macierzy przez jej producenta z wykorzystaniem połączenia internetowego i protokołu HTTPS.
    27.2. informowanie o wykorzystaniu zasobów dyskowych macierzy m.in. całkowitej pojemności przestrzeni dyskowej macierzy, wykorzystanej przestrzeni dyskowej, skonfigurowanej przestrzeni przydzielonej do serwerów i nie przydzielonej do serwerów oraz przestrzeni nie skonfigurowanej (wolnej);

27.3. monitorowanie zasobów wykorzystujących funkcjonalność thin-provisioning i ostrzeganie z wyprzedzeniem o możliwości wyczerpania zasobów;

27.4. monitorowanie stanu pracy par replikacyjnych, kopii migawkowych i klonów oraz funkcjonalności klastra active-active;

27.5. bieżące monitorowanie wydajności macierzy mierzonej w operacjach IOPS (zapis i odczyt), strumieniu MB/s (zapis i odczyt) oraz czasów odpowiedzi RT (zapis i odczyt) m.in. dla poszczególnych wolumenów logicznych, puli dyskowych oraz portów;

27.6. przygotowywanie raportów historycznych z okresu co najmniej 12 miesięcy zawierających informacje o wydajności mierzonej w IOPS i MB/s dla poszczególnych wolumenów logicznych i puli dyskowych.

27.7. wykrywanie błędów i izolowanie uszkodzeń, monitorowanie w czasie rzeczywistym.

27.8. zarządzanie macierzą z graficznego interfejsu użytkownika (GUI), linii komend (CLI) oraz programowego REST API.

27.9. monitoring i analizę wydajności systemu pamięci masowej (również macierzy firm trzecich), przełączników SAN oraz serwerów.

27.10. monitorowanie parametrów wydajnościowych w zakresie co najmniej IOPS, MB/s oraz czasów odpowiedzi RT i raportowanie przekroczenia zdefiniowanych progów.

27.11. korelację zmian parametrów wydajnościowych ze zmianami konfiguracji w środowisku.

27.12. generowanie alertów dla administratora przez e-mail, SMS, SNMP.

27.13. wykorzystanie zewnętrznych serwerów uwierzytelniania użytkowników: MS AD/LDAP.

27.14. automatyzacje zadań administracyjnych utworzoną w formie framework – graficznie przedstawienie zadań wykonywanych automatycznie zdefiniowany do uruchomienia poprzez wykrycie monitu (trigera).

27.15. automatyzowanie zmiany parametrów QOS dla wewnętrznej wirtualizacji zasobów udostępnianych do hostów/serwerów

27.16. zarzadzanie i konfigurowanie systemu kopii migawkowych wraz z repliką na inne ośrodki za pomocą GUI

Przełączniki FC usługi metroklastra – 4 sztuki	
Minimalne wymagania	
Obudowa	Przełącznik FC musi mieć wysokość maksymalnie 1U oraz zapewniać techniczną możliwość montażu w szafie Rack 19”. Wymagane dostarczenie i użycie szyn montażowych.
Ilość portów FC	Minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 8 portów FC przełącznika. Uruchomienie pozostałych 16 portów musi odbyć się bez konieczności wymiany urządzenia, jedynie poprzez dostawę licencji i modułów SFP.
Typ portów FC	Przełącznik FC musi być wykonany w technologii min. FC 32 Gb/s i zapewniać pracę portów FC z prędkościami 32, 16, 8, 4 Gb/s z funkcją auto-negocjacji prędkości.

	Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking" uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
Ilość modułów SFP oraz kabli	Przełącznik FC musi posiadać co najmniej 16 aktywnych portów objętych licencjami Do przełącznika należy dostarczyć wkładki: • min. 16 x SFP SWL 16 Gb/s, • min. 1x SFP+,LWL 16Gb/s, 10KM.
Gwarancja	Co najmniej 36 miesięcy od daty dostawy, Gwarancja świadczona w miejscu instalacji sprzętu, z czasem naprawy w kolejnym dniu roboczym od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej. Urządzenie musi być fabrycznie nowe. Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta. Gwarancja realizowana przez producenta lub jego autoryzowanego partnera serwisowego.
Parametry szczegółowe	
Konfiguracja portów	Przełącznik FC musi mieć możliwość instalacji modułów SFP LWL umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. Licencja na tę funkcjonalność nie jest wymagana na tym etapie postępowania. Rodzaj obsługiwanych portów: E, F, Diagnostic Port. Możliwość bezprzerwowej wymiany modułów SFP w trybie „na gorąco" (hot-swap). Wsparcie dla N_Port ID Virtualization (NPIV).
Trunking	Musi być zapewniona możliwość utworzenia logicznego połączenia „trunk" pomiędzy połączonymi przełącznikami o przepustowości 256 Gb/s (z wykorzystaniem minimum 8 portów 32Gb/s). Licencja nie jest wymagana na tym etapie postępowania.
Przepustowość	Sumaryczna przepustowość przełącznika FC musi wynosić minimum 768 Gb/s end-to-end full duplex.
Zoning	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN.
Bezpieczeństwo	Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: RADIUS, LDAP, SSHv2, SSL, HTTP, HTTPS, TACACS+, SCP, SFTP Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą, jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.

Zarządzanie przełącznikiem	Przełącznik FC musi zapewniać konfigurację przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP oraz statycznie. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany 10/100/1000 port Ethernet oraz serial port.

Doposażenie serwerów o karty HBA FC dla usługi metroklastra – 3 sztuki	
Karty HBA FC	Karta FC zgodna z: a) posiadanymi serwerami CISCO UCS C240 M4SX sn: FCH1945V1JL, FCH2147V250, FCH1945V1LP, b) dostarczanymi przełącznikami FC oraz c) macierzami dyskowymi, umożliwiająca poprawne działanie usługi metroklastra. Kara FC musi posiadać dwa porty obsługujące technologię FC z prędkościami 16, 8, 4 Gb/s z funkcją auto-negocjacji prędkości Kara musi posiadać możliwość pracy w topologii z przełącznikami (Fabric Connection) oraz w bezpośrednim połączeniu z dostarczaną macierzą (Direct Connection).
Gwarancja	Co najmniej 36 miesięcy od daty dostawy, Gwarancja świadczona w miejscu instalacji sprzętu, z czasem naprawy w kolejnym dniu roboczym od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej. Urządzenie musi być fabrycznie nowe. Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta. Gwarancja realizowana przez producenta lub jego autoryzowanego partnera serwisowego.

Usługi wdrożeniowe
Dostawa urządzeń, oprogramowania oraz licencji do lokalizacji wskazanych przez Zamawiającego. Opracowanie projektu technicznego wdrożenia. Opracowanie koncepcji i wykonanie migracji danych i aplikacji do środowiska metroklastra przy założeniu minimalizacji przestojów aplikacji i systemów Zamawiającego. Dla wskazanych przez Zamawiającego systemów dziedzinowych i usług krytycznych dla działania Urzędu migrację należy wykonać w sposób bezprzerwowy. Opracowanie i wykonanie zmian w politykach ochrony danych wykorzystując w pełni możliwości i zalety: usługi metroklastra chronionych retencją kopii wewnętrznych macierzy z udziałem automatycznych harmonogramów dostosowanych do RPO chronionych zasobów, integracji z posiadanym oprogramowaniem backupowym Veeam z wykorzystaniem trzech ośrodków, Przedstawienie do zatwierdzenia przez Zamawiającego zestawienia testów akceptacyjnych potwierdzających uzyskanie wymaganych parametrów niezawodności i wysokiej dostępności środowiska.

Przedstawienia do zatwierdzenia przez Zamawiającego zestawienia testów bezpieczeństwa wykazujących skuteczność ochrony wybranych systemów na ataki ransomware. Wdrożenie na podstawie opracowanego projektu technicznego usługi metroklastra opartej na dostarczonych przełącznikach FC, macierzach dyskowych oraz rozbudowanych o karty FC serwerach Zamawiającego. Rekonfiguracja klastra Hyper-V oraz danych na macierzach dyskowych. Oczekiwany efekt – dane z serwerów pracujących w klastrze Hyper-V są zapisywane i odczytywane jednocześnie na dwóch macierzach, awaria pojedynczej macierzy lub całej serwerowni nie powoduje przerwy w pracy aplikacji Zamawiającego ani utraty jakichkolwiek danych. Wykonanie warsztatów szkoleniowych w siedzibie Zamawiającego – minimum dwa dni robocze. Wykonanie audytu wszystkich kont administracyjnych systemów Windows/Linux oraz interfejsów zarządzających rozwiązania będącego przedmiotem umowy. Wymagane jest wykonanie raportu wszystkich kont administracyjnych. Celem audytu jest wykazanie, że wszystkie konta administracyjne zostały uwzględnione przy zmianie standardowych haseł dostarczonych przez producentów i nie są wykorzystywane w innych systemach podatnych na przejęcie tożsamości przez zastosowanie mechanizmów typu: pass-the-hash czy golden ticket. Wykonanie dokumentacji powykonawczej opisującej konfigurację poszczególnych parametrów każdego z elementów rozwiązania.

Usługi gwarancyjne
Gwarancja na okres min. 36 miesięcy. Przyjmowanie zgłoszeń 24/7 przez telefon, mail, elektroniczny system rejestracji zgłoszeń serwisowych Dostęp wyznaczonych osób do elektronicznego systemu rejestracji zgłoszeń. Czas reakcji na zgłoszenie – 4 h. Czas naprawy: awaria – następny dzień roboczy, usterka – 4 dni robocze. Aktualizacje firmware'ów dostarczonych urządzeń i instalacja poprawek/łatek bezpieczeństwa zgodnie z zaleceniami producenta przez cały okres gwarancji w trybie online.

CZĘŚĆ 2

„Dostawa systemu poczty elektronicznej z 5-letnim serwisem oraz wstępną konfiguracją, dysponującego wbudowanymi funkcjami ochrony przed spamem, ransomware i innymi zaawansowanymi atakami.”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup dostawa systemu poczty elektronicznej z 5 letnim serwisem oraz wstępną konfiguracją, dysponującego wbudowanymi funkcjami ochrony przed spamem, ransomware i innymi zaawansowanymi atakami.

2. Opis techniczny oferowanych urządzeń

Przedmiotem zamówienia jest zakup dostawa systemu poczty elektronicznej **wraz z 5 letnim serwisem** oraz wstępną konfiguracją, spełniającego poniższe wymagania:

1. Wymagania ogólne
System poczty elektronicznej musi być zrealizowany w postaci wirtualnej platformy, która musi posiadać możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.
System poczty elektronicznej musi pracować pod kontrolą dedykowanego systemu operacyjnego oraz wykorzystywać aktualizowane na bieżąco bazy zabezpieczeń.
System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.
System ochrony poczty musi być przystosowany do aktywnej współpracy oraz wymiany informacji o wykrytych podatnościach z urządzeniem firewall posiadanym przez Zamawiającego (Fortigate), w ramach kompatybilnych mechanizmów.
Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń
System musi obsługiwać co najmniej 4 interfejsy sieciowe
System musi obsługiwać przestrzeń dyskową o pojemności co najmniej 2 TB
System musi umożliwiać zapisanie konfiguracji systemu w pliku (lub plikach) zewnętrznym, z możliwością jej późniejszego odtworzenia
Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z następujących trybów: 1. Tryb Serwera 2. Tryb Gateway

3. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

2. Tryb Gateway / Tryb Transparentny

Funkcje ogólne

Dostarczany system ochrony poczty musi
zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 100 domen pocztowych.
2. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
3. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
4. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
5. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
6. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
7. Możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
8. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
9. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
10. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
11. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
12. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
13. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).

Kontrola antywirusowa i ochrona przed malware

W ww. zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W ww. zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

3. Tryb Serwer

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP oraz Radius.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 100 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.

15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.

13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

4. Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent, serwer.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra

5. Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

6. Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.

2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
4. System musi mieć możliwość integracji z posiadanymi przez zamawiającego urządzeniami Fortigate oraz FortiAnalyzer.
5. System musi mieć możliwość integracji z Fortinet Security Fabric

7. Certyfikaty

Dostarczony system powinien spełniać co najmniej dwa z poniższych certyfikacji:
1. VBSpam lub równoważny,
2. VB100 rated lub równoważny,
3. Common Criteria NDPP lub równoważny,
4. FIPS 140-2 Certified lub równoważny.

8. Serwisy i licencje

System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania przez okres 5 lat z aktualnych baz funkcji ochronnych producenta i serwisów. Dokument ten (licencję) należy dostarczyć na etapie realizacji zadania.
Muszą one obejmować: Kontrolę Antyspam, URL Filtering, kontrolę antywirusowa, ochronę typu Virus Outbrake, Sandbox w chmurze, ochronę typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise.

9. Gwarancja oraz wsparcie

System **musi być objęty** serwisem producenta przez **okres 5 lat**, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7
Wykonawca ze swojej strony gwarantuje:
1. Udzielenia kompleksowego wsparcia technicznego w zakresie instalacji systemu, jego konfiguracji oraz uruchomienia na produkcji, na platformie wskazanej przez Zamawiającego.
2. Wsparcie techniczne pierwszego kontaktu w języku polskim świadczone przez inżynierów certyfikowanych (w przypadku produktu firmy Fortinet wymagany jest certyfikat NSE 4), za pośrednictwem poczty elektronicznej oraz poprzez pomoc zdalną,
3. Zakładanie zgłoszeń serwisowych u producenta.
4. Doradztwo w zakresie konfiguracji.

10. Źródło pozyskania produktu

1. Produkt musi zostać zakupiony w oficjalnym kanale sprzedaży producenta.
2. Wykonawca powinien przedłożyć przed podpisaniem umowy oświadczenie producenta lub autoryzowanego dystrybutora producenta, potwierdzające autoryzację producenta w zakresie sprzedaży i serwisowania oferowanych rozwiązań.

11. Termin wdrożenia systemu

Wykonawca zobowiązany do wdrożenia systemu na produkcji na platformie wskazanej przez Zamawiającego w ciągu 45 dni od daty podpisania umowy

CZĘŚĆ 3

„Dostawa stacji roboczych o podwyższonym bezpieczeństwie”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 94 szt. nowych stacji roboczych o podwyższonym bezpieczeństwie wraz z oprogramowaniem systemowym i biurowym.

2. Opis techniczny oferowanych urządzeń

94 szt. nowych stacji roboczych o podwyższonym bezpieczeństwie

Przedmiotem zamówienia jest zakup i dostawa 94 sztuk nowych stacji roboczych, spełniających poniższe minimalne wymagania:

Konfiguracja sprzętowa komputera oraz obsługiwane technologie muszą pozwolić administratorom systemu na zdalne :	• zarządzanie i obsługę (KVM) komputera na poziomie sprzętowym • monitorowanie konfiguracji sprzętowej: procesora, dysków, pamięci RAM • pobieranie danych inwentaryzacyjnych • dostęp do BIOS i dziennika zdarzeń oraz zdalne uruchomienie/wyłączenie komputera. Funkcjonalności te muszą być dostępne niezależnie od stanu/obecności systemu operacyjnego. Komputery muszą być dostarczone wraz z oprogramowaniem niezbędnym do korzystania z ww. funkcjonalności.
Oznaczenie sprzętu	Komputer musi posiadać na obudowie LOGO producenta komputera umieszczone na obudowie w sposób trwały i odporny na zmywanie
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera.
Procesor wraz z chłodzeniem aktywnym	31000 pkt. według PassMark stan na dzień 15-12-2022
Płyta główna	1. złącza wewnętrzne: • 4 gniazda pamięci DDR4 z możliwością obsługi do 128GB • PCI-Express x1, 2x PCI-Express x16 • Serial ATA III

	• USB 3.2, USB 3.2 typ C • min.2x gniazdo M.2 PCIe 4.0 2. złącza zewnętrzne: • 1x Display Port • 1x HDMI • 1x RJ 45 • 2x USB • 3x USB 3.2 • 1x USB 3.2 typ C • 1x VGA • złącza audio 3. zintegrowana karta sieciowa 2.5Gb Ethernet 4. zintegrowana karta dźwiękowa 5. moduł szyfrujący TPM zintegrowany bądź dodatkowy dedykowany przez producenta spełniający wymagania systemu operacyjnego Microsoft Windows 11
Karta graficzna zintegrowana	Wydajność min. 2300 pkt. według PassMark stan na dzień 15-12-2022
Dysk M.2	• 512GB • 31000 pkt. według PassMark stan na dzień 15-12-2022
Pamięć RAM	• pojemność 32GB w maksymalnie dwóch modułach • częstotliwość pracy: 3200 MHz • dedykowany radiator
Zasilacz	• Moc: 600W • Certyfikat sprawności 80 Plus Gold • Aktywne PFC
Obudowa typu Tower	• ilość kieszeni 5.25 – maksymalnie 1 • ilość kieszeni 3.5 wew. - 1 • ilość kieszeni 2.5 wew. - 1 • złącza na przednim panelu: 2x USB 3.0, złącza audio • zamontowane wentylatory: 2x 120mm z możliwością montażu kolejnych dwóch
Monitor	• przekątna 22”-24” • rozdzielczość nominalna: 1920x1080 • częstotliwość odświeżania: 144Hz • wbudowane głośniki • złącza: DisplayPort, HDMI
Klawiatura i mysz (zestaw jednego producenta)	• zestaw przewodowy USB • kolor czarny • typ klawiatury: tradycyjna z oddzielną klawiaturą numeryczną • typ myszy: optyczna lub laserowa,

	uniwersalna (dla prawo i leworęcznych)
System operacyjny (**indywidualny klucz dla każdej stacji roboczej)**	Microsoft Windows Pro 11 64 bit PL lub równoważny*
Pakiet biurowy (**indywidualny klucz dla każdej stacji roboczej)**	MS Office 2021 Home & Business PL lub równoważny**
Komputer w oferowanej konfiguracji sprzętowej musi osiągać w teście **BAPCo SYSmark 25** wyniki:	• Overall - nie mniej niż 1835 pkt • Productivity – nie mniej niż 1767 pkt
Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk szczegółowego raportu z testów wydajności BAPCo SYSmark 25, dla komputera w konfiguracji identycznej z oferowaną (jeśli będzie ich kilka to każdej z komfiguracji). Zamawiający wymaga aby test wydajności SYSmark 25 został wykonany w konfiguracji całego komputera identycznej z wymaganą oraz przy rozdzielczości ekranu 1920 x 1080 i innymi ustawieniami zgodnymi z zaleceniami producenta testu, tj. na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCo oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych testów Wykonawca może zostać wezwany przy dostawie do wykonania w obecności Zamawiającego, na dwóch losowo wskazanych przez Zamawiającego komputerach, testów ich wydajności, zgodnie z powyższymi wymaganiami, potwierdzającymi wymagane wyniki wydajnościowe. **Składany raport nie może być wykonany wcześniej niż 45 dni przed złożeniem oferty**. Raport należy dostarczyć wraz z ofertą.	

Zalecane jest by komputery posiadały jednolitą wersję komponentów dla całej puli urządzeń objętych zamówieniem. W przypadku komputerów o różnych konfiguracjach testy BAPCo muszą być wykonane dla każdej różnej konfiguracji sprzętowej komputera.

ZAŁĄCZNIKI TABEL Z PARAMETRAMI WARTOŚCI PASSMARK ZOSTAŁY DOŁĄCZONE DO OPZ JAKO ZAŁĄCZNIK NR 1-3 DO OPZ

*** Oprogramowanie typu MS Windows 11 Professional 64 bit PL lub równoważne**, spełniające poniższe warunki:

1) System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika;
2) System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016; MS Visio 2010, 2016; MS Project 2010, 2016; EMID, AutoCAD, Microsoft Visual Studio Professional. Nie jest dopuszczalne uruchamianie wymienionych aplikacji poprzez mechanizm wirtualizacji;
3) System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
   a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych;
4) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim;
5) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
6) Wbudowany system pomocy w języku polskim;

7) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim;
8) 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;
9) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego;
10) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego;
11) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami;
13) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);
14) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
15) Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
16) Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
17) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe;
18) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;
19) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:
    a) poziom menu,
    b) poziom otwartego okna systemu operacyjnego;
20) System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
21) Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;
22) Obsługa standardu NFC (near field communication);
23) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24) Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25) Mechanizmy logowania do domeny w oparciu o:
    a) login i hasło,
    b) karty z certyfikatami (smartcard),
    c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM);
26) Mechanizmy wieloelementowego uwierzytelniania;
27) Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu;
28) Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec;

29) Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
30) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
31) Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
32) Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
33) 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;
34) Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;
35) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
36) Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
37) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
38) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci;
39) 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.);
40) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
41) Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych;
42) Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika;
43) Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB;
44) Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych;
45) Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych;
46) Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

**** Oprogramowanie MS Office 2021 Home & Business 64 bit PL lub równoważne**, spełniające poniższe warunki:
Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1) Musi zawierać co najmniej następujące komponenty:
   a) edytor tekstu,
   b) arkusz kalkulacyjny,
   c) program do przygotowywania i prowadzenia prezentacji,

d) program do zarządzania informacją przez użytkownika (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
e) program do integrowania z wieloma źródłami danych;

2) Wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi;
3) Dostępna pełna polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej pomocy technicznej;
4) Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, accdb, w tym obsługa formatowania bez utraty parametrów i cech użytkowych (zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów);
5) Wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach wytworzonych w MS Office 2016, 2019 bez utraty danych oraz bez konieczności przerabiania dokumentów;
6) Możliwość zapisywania wytworzonych dokumentów bezpośrednio w formacie PDF;
7) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory;
8) Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich elementów;
9) Możliwość jednoczesnej pracy wielu użytkowników na udostępnionym dokumencie arkusza kalkulacyjnego;
10) Posiadać pełną kompatybilność z systemami operacyjnymi: MS Windows 10 (64-bit) lub MS Windows 11 (64-bit).

CZĘŚĆ 4

„Dostawa komputerów przenośnych”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 5 szt. nowych komputerów przenośnych (laptopów) do zarządzania serwerami i siecią IT.

2. Opis techniczny oferowanych urządzeń

Przedmiotem zamówienia jest dostawa 5 szt. nowych komputerów przenośnych (laptopów) do zarządzania serwerami i siecią IT, spełniających poniższe minimalne wymagania:

Procesor	28700 pkt. według PassMark stan na dzień 15-12-2022
Pamięć RAM	16GB – 4800 MHz z możliwością rozbudowy do min. 32 GB
Ekran	• 15,6”-16”, • rozdzielczość nominalna 2560x1440, • częstotliwość odświeżania 240 Hz
Dysk SSD M.2 PCIe	1000GB
Karta graficzna	Wydajność 18300 pkt. według PassMark stan na dzień 15-12-2022
Złącza zewnętrzne	2x USB 3.2; 1x USB type C; 1x wyjście HDMI; 1x RJ45
Komunikacja	Bluetooth; Wi-Fi 6, LAN 1GB/s
Pozostałe cechy	• Wbudowane głośniki stereo, • wbudowana kamera internetowa min. 1 Mpix; szyfrowanie TPM, • podświetlana klawiatura
Gwarancja	• minimum 24 miesiące

ZAŁĄCZNIKI TABEL Z PARAMETRAMI WARTOŚCI PASSMARK ZOSTAŁY DOŁĄCZONE DO OPZ JAKO ZAŁĄCZNIK NR 1-3 DO OPZ

CZĘŚĆ 5

„Dostawa serwera i stacji roboczych na potrzeby Miejskiego Ośrodka Kultury”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa:

1) 2 szt. nowych stacji roboczych;
2) 1 szt. specjalnej jednostki komputerowej wraz z zasilaczem awaryjnym UPS do obsługi portalu wewnętrznego i portali zewnętrznych;
3) 1 szt. nowego serwera domeny wraz z zasilaczem awaryjnym UPS.

2. Opis techniczny oferowanych urządzeń

3.1. 2 szt. nowych stacji roboczych

Przedmiotem zamówienia jest zakup i dostawa dwóch fabrycznie nowych stacji roboczych, spełniających poniższe minimalne wymagania:

Procesor wraz chłodzeniem aktywnym	nie słabszy niż 17000 pkt. według PassMark (https://www.cpubenchmark.net) na dzień 15-12-2022
Pamięć RAM	16 GB w maksymalnie dwóch modułach, DDR4 taktowana 3000MHz (efektywnie) z dedykowanym radiatorem
Płyta główna	• Złącza wewnętrzne: -4x gniazda pamięci DDR4 z możliwością obsługi do 128GB -1x gniazda M.2 PCIe NVMe 4.0 x4 -1x gniazda M.2 PCIe NVMe 3.0 x4 -1x PCIe 3.0 x16 (elektrycznie x16) -1x PCIe 3.0 x16 (elektrycznie x4) -1x PCIe 3.0 x1 -4x wentylatora obudowy -2x SATA • Złącza zewnętrzne: -1x złącze 8P8C na tyle obudowy -2x USB 3.2 Gen. 1 na tyle obudowy -1x USB 3.2 Gen. 2 na tyle obudowy -1x USB Gen 2 Typu C na tyle obudowy -2x złącze 3.2 Gen. 1 na przodzie obudowy -złącze głośników • Zintegrowana karta sieciowa 2,5Gbps • Zintegrowana karta dźwiękowa • Moduł TPM 2.0 • Zgodność z Windows 11

Dysk	• 500GB min. 33000 pkt wg. https://www.harddrivebenchmark.net na dzień 15-12-2022 • szyfrowanie sprzętowe dysku
Karta graficzna	• minimum 2500 pkt PassMark, https://www.videocardbenchmark.net na dzień 15-12-2022 • obsługa Windows 11 • złącza 1xHDMI, 1xDisplayPort
Obudowa	• Tower (wolnostojąca) • 2x złącze USB 3.2 Gen. 1 na przodzie obudowy • zamontowane 2 wentylatory i możliwość montażu kolejnych 2 • złącza słuchawek i mikrofonu na przodzie obudowy • możliwość montażu w zatoki wewnętrzne 2x dysk 3,5” • filtry przeciwkurzowe w miejscach poboru powietrza przez obudowę
Zasilacz	Min.550W z certyfikatem 80 Plus Gold
System operacyjny:	Microsoft Windows Pro 11 Professional lub równoważny*
Monitor	• min. 23,5” • złącze HDMI, • wbudowane głośniki, • matryca IPS, 75 Hz
Klawiatura i mysz	• przewodowa klawiatura + mysz • klawiatura z osobnym blokiem numerycznym • kolorystyka stonowana nie wyróżniająca się między elementami zestawu

ZAŁĄCZNIKI TABEL Z PARAMETRAMI WARTOŚCI PASSMARK ZOSTAŁY DOŁĄCZONE DO OPZ JAKO ZAŁĄCZNIK NR 1 DO OPZ

*** Oprogramowanie typu MS Windows 11 Professional 64 bit PL lub równoważne**, spełniające poniższe warunki:

1) System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika;
2) System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016; MS Visio 2010, 2016; MS Project 2010, 2016; EMID, AutoCAD, Microsoft Visual Studio Professional. Nie jest dopuszczalne uruchamianie wymienionych aplikacji poprzez mechanizm wirtualizacji;
3) System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
   a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych;
4) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim;
5) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
6) Wbudowany system pomocy w języku polskim;
7) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim;
8) 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;
9) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego;
10) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego;
11) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami;
13) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);
14) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
15) Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
16) Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
17) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe;
18) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;
19) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:
a) poziom menu,
b) poziom otwartego okna systemu operacyjnego;
20) System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
21) Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;
22) Obsługa standardu NFC (near field communication);
23) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24) Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25) Mechanizmy logowania do domeny w oparciu o:
a) login i hasło,

b) karty z certyfikatami (smartcard),
c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM);
26) Mechanizmy wieloelementowego uwierzytelniania;
27) Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu;
28) Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec;
29) Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
30) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
31) Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
32) Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
33) 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;
34) Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;
35) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
36) Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
37) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
38) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci;
39) 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.);
40) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
41) Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych;
42) Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika;
43) Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB;
44) Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych;
45) Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych;
46) Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

3.2. 1 szt. specjalnej jednostki komputerowej wraz z zasilaczem awaryjnym UPS do obsługi portalu wewnętrznego i portali zewnętrznych

Przedmiotem zamówienia jest zakup i dostawa fabrycznie nowej stacji roboczej wraz z zasilaczem awaryjnym UPS. Podzespoły stacji roboczej muszą spełniać poniższe minimalne wymagania:

Procesor wraz z chłodzeniem aktywnym	nie słabszy niż 27000 pkt. według https://www.cpubenchmark.net stan na dzień 15-12-2022
Płyta główna	• Złącza wewnętrzne: -4x gniazda pamięci DDR5 z możliwością obsługi do 128GB -3x gniazda M.2 PCIe NVMe 4.0 x4 -1x PCIe 5.0 x16 (elektrycznie x16) -1x PCIe 3.0 x16 (elektrycznie x4) -6x wentylatora obudowy • Złącza zewnętrzne: -1x złącze 8P8C -2x USB 3.2 Gen. 1 na tyle obudowy -1x USB 3.2 Gen. 2 na tyle obudowy -1x USB Gen 2x2 Typu C -2x złącze 3.2 Gen. 1 na przodzie obudowy -złącze głośników • Zintegrowana karta sieciowa 2,5Gbps • Zintegrowana karta dźwiękowa • Moduł TPM 2.0 • Zgodność z Windows 11
Pamięć RAM	16 GB w maksymalnie dwóch modułach, DDR5 taktowana 4800MHz (efektywnie) z dedykowanym radiatorem
Dysk	• Min. 1TB 38000 pkt. wg https://www.harddrivebenchmark.net stan na dzień 15-12-2022 • sprzętowe szyfrowanie dysku
Karta graficzna	• minimum 18000 pkt wg PassMark https://www.videocardbenchmark.net na dzień 15-12-2022 • obsługa Windows 11
Obudowa	• Tower (wolnostojąca) • 2x złącze USB 3.2 Gen. 1 na przodzie obudowy - zamontowane 3 wentylatory i możliwość montażu kolejnych 3 • złącza słuchawek i mikrofonu na przodzie obudowy • możliwość montażu w zatoki wewnętrzne 2x dysk 3,5”

	• filtry przeciwkurzowe w miejscach poboru powietrza przez obudowę
Zasilacz	Min. 750W z certyfikatem 80 Plus Gold
System operacyjny:	Microsoft Windows Pro 11 Professional lub równoważny*
Klawiatura i mysz	• przewodowa klawiatura + mysz • klawiatura z osobnym blokiem numerycznym • kolorystyka stonowana nie wyróżniająca się między elementami zestawu
UPS	• 850 VA, 800W • złącza 2xSchuko, 1xUSB • wyświetlacz kontrolny napięć I naładowania

ZAŁĄCZNIKI TABEL Z PARAMETRAMI WARTOŚCI PASSMARK ZOSTAŁY DOŁĄCZONE DO OPZ JAKO ZAŁĄCZNIK NR 1-3 DO OPZ

*** Oprogramowanie typu MS Windows 11 Professional 64 bit PL lub równoważne**, spełniające poniższe warunki:

1) System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika;
2) System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016; MS Visio 2010, 2016; MS Project 2010, 2016; EMID, AutoCAD, Microsoft Visual Studio Professional. Nie jest dopuszczalne uruchamianie wymienionych aplikacji poprzez mechanizm wirtualizacji;
3) System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
   a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych;
4) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim;
5) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
6) Wbudowany system pomocy w języku polskim;
7) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim;
8) 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;
9) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego;
10) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego;
11) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami;

13) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);
14) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
15) Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
16) Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
17) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe;
18) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;
19) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:
    a) poziom menu,
    b) poziom otwartego okna systemu operacyjnego;
20) System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
21) Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;
22) Obsługa standardu NFC (near field communication);
23) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24) Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25) Mechanizmy logowania do domeny w oparciu o:
    a) login i hasło,
    b) karty z certyfikatami (smartcard),
    c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM);
26) Mechanizmy wieloelementowego uwierzytelniania;
27) Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu;
28) Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec;
29) Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
30) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
31) Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
32) Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
33) 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;
34) Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;
35) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;

36) Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
37) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
38) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci;
39) 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.);
40) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
41) Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych;
42) Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika;
43) Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB;
44) Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych;
45) Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych;
46) Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

3.3. 1 szt. nowego serwera domeny wraz z zasilaczem awaryjnym UPS

Przedmiotem zamówienia jest zakup i dostawa fabrycznie nowego serwera domeny wraz z zasilaczem awaryjnym UPS spełniającego poniższe wymagania:

Wymagany zdalny dostęp na poziomie sprzętowym (bez potrzeby obecności systemu operacyjnego)	• uruchomienie i wyłączenie urządzenia • wykonanie pełnego cyklu rozruchowego (zimny rozruch) • dostęp do obecnej konfiguracji sprzętowej procesora, RAM i dysków • zmiana konfiguracji w sprzętowym kontrolerze RAID
Procesor wraz z chłodzeniem aktywnym	16900 pkt. wg PassMark (https://www.cpubenchmark.net) stan na dzień 15-12-2022
Płyta główna	• Złącza wewnętrzne: 4 gniazda pamięci DDR4 z możliwością obsługi do 128GB 1x PCI-e x16 (elektrycznie) 2x PCI-e x4 (elektrycznie)

	• Złącza zewnętrzne: -1x złącze D-Sub -2x złącze 8P8C -1x złącze USB 3.0 na tyle obudowy -2x złącze USB 2.0 na tyle obudowy -1x złącze USB 3.0 na przodzie obudowy • zintegrowana karta sieciowa 2x1Gbps
Pamięć RAM	• 16 GB w maksymalnie dwóch modułach DDR4 taktowana 3200 MHz (efektywnie)
Dyski	2x 500GB RAID 1 minimum 4800 pkt wg PassMark dla każdego dysku osobno https://www.harddrivebenchmark.net) stan na dzień 15-12-2022 2x 4TB RAID 1
Kontrolery	jako osobny moduł Obsługiwane poziomy RAID: 0, 1, 10,
Obudowa	• Tower (wolnostojąca) • możliwość montażu 2 zasilaczy hot-plug • możliwość montażu 4szt. dysków zamiennie (nawet po ew. zmianie kieszeni) lub po 4 szt. osobno w formatach 2,5” i 3,5” • 1x złącze USB 3.0 na przodzie obudowy
Zasilacz	minimum 1szt. 600 W certyfikat 80 Plus Platinum
System operacyjny:	Microsoft Server 2022 Essentials lub równoważny***
Klawiatura i mysz	• przewodowa klawiatura + mysz • klawiatura z osobnym blokiem numerycznym • kolorystyka stonowana nie wyróżniająca się między elementami zestawu
UPS	• 1000 VA, 600W • złącza 4xIEC-C13 lub Schuko, 1xUSB • wyświetlacz kontrolny napięć I naładowania • typ obudowy tower • czas podtrzymywania (obciążenie 100%): 9min

ZAŁĄCZNIKI TABEL Z PARAMETRAMI WARTOŚCI PASSMARK ZOSTAŁY DOŁĄCZONE DO OPZ JAKO ZAŁĄCZNIK NR 1-3 DO OPZ

*** Przez system równoważny do Microsoft Windows Server 2022 Essentials Zamawiający rozumie system spełniający następujące wymagania funkcjonalne:

1. Wspierający graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.
2. Zapewniający natywne wsparcie dla środowiska .NET Framework 4.8.

3. Zapewniający możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory.
4. System operacyjny musi wspierać pracę domenową.
5. System operacyjny musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP.
6. System operacyjny musi posiadać możliwość uruchomienia serwera DNS.
7. Licencja na system operacyjny zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 1 środowiska wirtualnego za pomocą wbudowanego mechanizmy wirtualizacji, bez konieczności zakupu dodatkowych licencji.
8. Umożliwiający obsługę minimum 48 TB pamięci RAM.
9. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu.
10. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
11. Zapewniający pełne wsparcie dla podzespołów zainstalowanych w zamawianym sprzęcie komputerowym (przy ew. wykorzystaniu sterowników od odpowiednich producentów podzespołów).
12. Licencja na system operacyjny musi być bez ograniczeń czasowych.

CZĘŚĆ 6

„Rozbudowa środowiska serwerowego poprzez dostawę oprogramowania serwerowego”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest rozbudowa środowiska serwerowego poprzez dostawę oprogramowania serwerowego i licencji dostępowych do posiadanych serwerów.

2. Opis techniczny oferowanego oprogramowania

I. <u>Dostawa oprogramowania Microsoft Windows Server Datacenter 2022 lub równoważnego oprogramowania</u>.

Licencje muszą:

1) pozwalać na za licencjonowanie czterech fizycznych serwerów posiadających:
   a) Serwer nr 1 - Dwa procesory o 6 rdzeniach każdy (2x CPU, 6 rdzeni na CPU),
   b) Serwer nr 2 - Dwa procesory o 12 rdzeniach każdy (2x CPU, 12 rdzeni na CPU),
   c) Serwer nr 3 - Dwa procesory o 14 rdzeniach każdy (2x CPU, 14 rdzeni na CPU),
   d) Serwer nr 4 - Dwa procesory o 6 rdzeniach każdy (2x CPU, 6 rdzeni na CPU);
2) być nieograniczone czasowo ani funkcjonalnie;
3) pozwalać na uruchomienie nieograniczonej liczby instancji systemów operacyjnych (OSE) i kontenerów Hyper-V w obrębie serwera fizycznego;
4) uprawniać do instalacji wcześniejszych wersji systemu Windows Serwer tzn. Windows Server 2012 R2, Windows Server 2016, Windows Serwer 2019;
5) mieć możliwość ich przenoszenia na inne serwery fizyczne;
6) być zarejestrowane na dane Zamawiającego;
7) być dostępne w portalu Microsoft 365 Admin Center.

W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie Przedmiotu Zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w SIWZ, w szczególności w zakresie:

1. Współpraca z procesorami o architekturze x64.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny zgodnie z wypisanymi wcześniej wymaganiami dla licencji .
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2019.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.

10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych (dla wersji Standard) oraz na nieograniczonej ilości maszyn wirtualnych w ramach licencjonowanego hosta (dla wersji Datacenter).
14. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
15. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
16. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
17. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
18. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
19. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
20. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
21. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
22. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
23. Możliwość wykorzystania standardu http/2.
24. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
25. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
26. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
27. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
28. Mechanizmy logowania w oparciu o:
    a. login i hasło,
    b. karty z certyfikatami (smartcard),

c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).

29. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    a. kreślonych grup użytkowników,
    b. zastosowanej klasyfikacji danych,
    c. centralnych polityk dostępu w sieci,
    d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
30. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
31. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
32. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
33. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
34. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
35. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        a) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        b) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        d) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        a) Dystrybucję certyfikatów poprzez http,
        b) Konsolidację CA dla wielu lasów domeny,
        c) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        d) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f. Szyfrowanie plików i folderów.

g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)

h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi

i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,

j. Serwis udostępniania stron WWW

k. Wsparcie dla protokołu IP w wersji 6 (IPv6).

l. Wsparcie dla algorytmów Suite B (RFC 4869).

m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.

o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.

q. Mechanizmy wirtualizacji mające wsparcie dla:

a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

b) obsługi ramek typu jumbo frames dla maszyn wirtualnych.

c) obsługi 4-KB sektorów dysków,

d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,

e) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

f) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw.
trunk mode)

g) możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

r. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.

s. Wsparcie dla rozwiązania Kubernetes.

t. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

u. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek
(Multipath).

v. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.

w. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

x. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

y. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF

z. Mechanizm konfiguracji połączenia VPN do platformy Azure.

aa. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.

bb. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.

cc. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

dd. Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Enterprise).

36. W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.

37. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

II. **<u>Przedmiotem zamówienia jest dostawa 250 szt. licencji dostępowych Microsoft Windows Server 2022 Device CAL do posiadanych serwerów</u> Zamawiają**cego, dających prawo dostępu z 250 sztuk stacji roboczych do serwerów pracujących pod kontrolą systemów operacyjnych Microsoft Windows Server 2012, 2016, 2019 i 2022.

W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie Przedmiotu Zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w SIWZ, w szczególności w zakresie:

1) warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania Microsoft,
2) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Microsoft Windows Server funkcjonującym u Zamawiającego,
3) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
4) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie Microsoft Windows Server,
5) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem MICROSOFT WINDOWS SERVER 2022 DEVICE CAL ,
6) w przypadku zaproponowania oprogramowania równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji

zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin,

7) w przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie,
8) w przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego oraz dostarczy inne rozwiązana spełniające wymagania OPZ,
9) oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia/gwarancji producentów używanego i współpracującego z nim oprogramowania u Zamawiającego,
10) oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty,
11) zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności osiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

Wymagania organizacyjne:

Dostarczone klucze licencyjne muszą zostać przypisane do konta Zamawiającego (Urzędu Miejskiego w Pabianicach). Dane konta (Tenanta) zostaną przekazane Wykonawcy po rozstrzygnięciu postępowania i wyłonieniu Wykonawcy.

Na potrzeby odbioru zostanie zweryfikowane czy na portalu licencyjnym, na koncie Zamawiającego, pojawił się nowy klucz licencyjny na komplet dostarczanych licencji wraz ze wsparciem technicznym.

CZĘŚĆ 7

„Dostawa oprogramowania antywirusowego”

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 12 szt. oprogramowania antywirusowego.

2. Opis techniczny oferowanego oprogramowania

Przedmiotem zamówienia jest zakup i dostawa licencji oprogramowania antywirusowego spełniającego poniższe minimalne wymagania:

3 licencje na okres 3 lat	Posiadające: • moduł bezpiecznych przelewów, firewall, • możliwość blokowania urządzeń peryferyjnych (pendrive) • Antywirus i antyspyware • Antyphishing • Ochrona przed ransomware • Ochrona przed zagrożeniami bazującymi na skryptach • Skaner UEFI • Blokadę programów typu exploit
9 licencji na okres 3 lat	Posiadające: • możliwość blokowania urządzeń peryferyjnych (pendrive) • Antywirus i antyspyware • Antyphishing • Ochrona przed ransomware • Ochrona przed zagrożeniami bazującymi na skryptach • Skaner UEFI • Blokada programów typu exploit