Załącznik nr 3 do SWZ

I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO

1. **Zakres przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa licencji, oprogramowania, fabrycznie nowego sprzętu komputerowego, wdrożenie systemów i rozwiązań teleinformatycznych mających na celu podniesienie poziomu cyfryzacji urzędu w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczące realizacji projektu grantowego „**Cyfrowa Gmina**" o numerze **POPC.05.01.00-00-0001/21-00**

Kody Wspólnego Słownika Zamówień: kody CPV dla części I, II, III i IV:

- 30236000-2 – Różny sprzęt komputerowy
- 31710000-6 – Sprzęt elektroniczny
- 32422000-7 – Elementy składowe sieci
- 48000000-8 – Pakiety oprogramowania i systemy informatyczne
- 71356300-1 – Usługi wsparcia technicznego
- 72263000-6 – Usługi wdrażania oprogramowania

Szczegółowy zakres projektu składa się z następujących części:

1) **Część I - Dostawa szafy teleinformatycznej Rack 42U z wyposażeniem oraz dodatkowymi akcesoriami – 1 szt.**

- Infrastruktura zostanie zainstalowana w nowej w pełni wyposażonej, profesjonalnej szafie teleinformatycznej typu Rack o wysokości 42U. Zakup szafy umożliwi zainstalowanie sprzętu w sposób profesjonalny, bezpieczny oraz zapewnieni dostęp jedynie dla osób uprawnionych. Kod główny CPV 31213300-5 – Szafy kablowe

2) **Część II - Dostawa serwerów (serwer typ 1 i 2, serwer backupu) wraz z oprogramowaniem z usługą wdrożenia – 3 szt.**

W celu zminimalizowania przestojów i zapewnienia nieprzerwanej pracy w przypadku awarii, Zamawiający zaplanował zakup dwóch serwerów (podstawowego i zapasowego) wraz z licencjami dla serwerów fizycznych na serwerowy system operacyjny oraz wymagane licencje dostępowe, których zadaniem jest udostępnianie usług oraz zabezpieczenie ciągłości pracy poprzez pracę w trybie replikacji maszyn virtualnych. Dodatkowo w celu zapewnienia bezpieczeństwa i ochrony danych w sieci lokalnej zaplanowano zakup serwera backupu, dzięki któremu możliwe będzie wykonywanie bezpiecznych, integralnych kopii zapasowych. Backup będzie wykonywany dla danych z systemów dziedzinowych, maszyn wirtualnych oraz danych użytkowników. Uzupełnieniem funkcjonalności serwera do backupu będzie zakup licencji na oprogramowanie do backupu danych, która zautomatyzuje cały proces zapewniając jego cykliczność i logowanie wykonanych zadań.

Celem prac wdrożeniowych jest przygotowanie do eksploatacji kompletnego środowiska teleinformatycznego, na potrzeby realizacji projektu, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. W ramach zadania wymagane jest wykonanie

usługi instalacji, konfiguracji oraz uruchomienia dostarczonych urządzeń. Kod główny CPV 48820000-2 – Serwery.

3) **Część III - Dostawa, konfiguracja oraz uruchomienie urządzenia UTM – 1 kpl.**
Głównym elementem chroniącym dostęp do zasobów sieciowych będzie firewall sprzętowy. Zakup profesjonalnej zapory sieciowej zapewni ochronę przed cyberatakami z zewnątrz, zabezpieczy również lokalną sieć wraz z wszystkimi urządzeniami, które się w niej znajdują. Urządzenie to umożliwi filtrowanie oraz logowanie ruchu www, ochronę przed spamem, ochronę przed szkodliwym oprogramowaniem (np. malware, ransomware), a w przypadku konieczności pracy zdalnej zabezpieczy połączenie VPN, za pomocą którego realizowane będzie połączenie zdalne. Kod główny CPV 32420000-3 – Urządzenia sieciowe.

4) **Część IV - Dostawa, konfiguracja, uruchomienie skanera dokumentów oraz wdrożenie oprogramowania do skanowania – 1 kpl.**
Zamawiający w celu usprawnienia pracy z systemem obiegu dokumentów funkcjonującym z Urzędzie Gminy zaplanował zakup nowoczesnego skanera szczelinowego pozwalającego na skanowanie dowolnych dokumentów (dowolny format, gramatura papieru, itp.) dwustronnie w jednym przebiegu skanowania z możliwością rozpoznawania znaczników dokumentów. Pozwoli to na wydatne skrócenie wprowadzania dokumentów do systemu SOD i zwiększenie wydajności pracy. Główny kod CPV 30216110-0 - Skanery komputerowe.

2. Ogólne wymagania Zamawiającego

Niniejszy dokument ma celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawy oraz usługi teleinformatyczne, których podstawowym celem jest podniesienie poziomu cyfryzacji Urzędu oraz bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa). Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych oraz wskazuje technologie, które powinny być wykorzystane tak, aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.
Opisane w dokumencie wymagania należy traktować jako **podstawowe i minimalne**, a te które zostały określone jako dodatkowe traktować należy jako nieobowiązkowe (fakultatywne).

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3

ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne".

W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

3. **Wymagania ogólne dotyczące sprzętu:**
   1) Wszystkie dostarczone urządzenia muszą być fabrycznie nowe (wyprodukowane w roku 2022), bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wcześniejszych wystaw bądź prezentacji.
   2) Dostarczone urządzenia muszą być wykonane w ramach bezpiecznych technologii oraz być wolne od obciążeń prawami osób trzecich, a także muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej.
   3) Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.
   4) Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE oraz powinny posiadać certyfikację oraz oznaczenie CE.
   5) Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów wyposażenia lub dodatkowych akcesoriów.
   6) Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.
   7) W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy urządzeń, w szczególności podzespoły montowane przez producenta były przez niego certyfikowane. Wykonawca nie będący producentem oferowanego sprzętu nie może samodzielnie dokonywać modyfikacji sprzętu i wprowadzać zmian w fabrycznej konfiguracji. Zamawiający nie dopuszcza dostawy urządzeń modyfikowanych przez sprzedawcę oraz nie dopuszcza modyfikacji na linii produkcyjnej dystrybutora.

4. **Wymagania ogólne dotyczące oprogramowania:**
   Wykonawca zobowiązany jest dostarczyć Zamawiającemu:
   1) drukowane certyfikaty licencyjne wystawione przez producenta oprogramowania, o ile nie są dostępne w formie elektronicznej;
   2) nośniki instalacyjne oprogramowania, o ile nie są dostępne w formie elektronicznej;
   3) adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze wsparcia technicznego świadczonego przez producenta oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
   4) zestawienie dostarczonych Zamawiającemu pozycji w zakresie oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa),

okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego,

5) standardowe warunki licencyjne producenta oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6) standardowe warunki wsparcia technicznego producenta oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7) oświadczenie producenta oprogramowania bądź autoryzowanego dystrybutora dostarczonego oprogramowania, potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki wsparcia technicznego;
8) dostarczone oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności, wymagane przez producenta oprogramowania w zależności od dostarczanej wersji;
9) Zamawiający zastrzega sobie prawo do weryfikacji oprogramowania na etapie dostawy, również pod kątem jego legalności. W ramach procedury odbioru, Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji legalności i oryginalności oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny. W przypadku wykrycia, że dostarczone w ramach umowy oprogramowanie nie jest nowe, było już używane lub było już wcześniej aktywowane Zamawiający odmówi przyjęcia oprogramowania (lub sprzętu z zainstalowanym oprogramowaniem) i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

5. **<u>Wymagania ogólne dotyczące realizacji dostawy.</u>**
   1) Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
   2) Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, m.in. rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
   3) Wykonawca, co najmniej na 3 dni przed dniem planowanej dostawy sprzętu, dokona jej awizacji, to znaczy skontaktuje się z Zamawiającym w celu ustalenia miejsca i potwierdzenia konkretnego terminu dostawy.
   4) Dostawa sprzętu odbędzie się w dniu roboczym, od poniedziałku do czwartku, w godzinach 8:00 - 14:00, transportem zapewnionym przez Wykonawcę, na jego koszt i ryzyko wraz z wniesieniem do miejsca wskazanego przez Zamawiającego.
   5) Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
   6) Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń oraz wszelką dokumentację dostarczoną przez producenta sprzętu.

6. **<u>Wymagania gwarancyjne.</u>**

1) O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta sprzętu bądź udzielona przez autoryzowany serwis gwarancyjny producenta sprzętu. Serwis gwarancyjny musi być świadczony przez autoryzowany serwis producenta lub przez samego producenta i powinien być świadczony w miejscu instalacji sprzętu, Zamawiający nie dopuszcza udzielenia gwarancji Wykonawcy na sprzęt. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego (chyba że zapisy szczegółowe stanowią inaczej).
2) Gwarantowany czas naprawy nie może być dłuższy niż 5 dni roboczych (chyba że zapisy szczegółowe stanowią inaczej). W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 30 dni roboczych od momentu zgłoszenia usterki.
3) Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
4) Oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej).

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne zawarte w dalszej części OPZ.

7. **Miejsce instalacji i uruchomienia Systemu Informatycznego (instalacji sprzętu i oprogramowania).**
Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części OPZ, w budynku urzędu w miejscach wskazanych przez Zamawiającego.

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

8. **Zamawiający dopuszcza możliwość składania ofert częściowych:**
1) Przedmiot zamówienia w zakresie części nr 1 dotyczy:
Dostawy szafy teleinformatycznej Rack 42U z wyposażeniem oraz dodatkowymi akcesoriami – 1 szt.
2) Przedmiot zamówienia w zakresie części nr 2 dotyczy:
Dostawy serwerów wraz z oprogramowaniem z usługą wdrożenia – 3 szt.
3) Przedmiot zamówienia w zakresie części nr 3 dotyczy:
Dostawy, konfiguracji oraz uruchomienia urządzenia UTM – 1 kpl.
4) Przedmiot zamówienia w zakresie części nr 4 dotyczy:
Dostawa, konfiguracja, uruchomienie skanera dokumentów oraz wdrożenie oprogramowania do skanowania.

Każdy z wykonawców może złożyć ofertę na wybraną przez siebie część lub części zamówienia.
Ofertę można składać na wszystkie części.
Zamawiający nie ogranicza liczby części zamówienia, którą można udzielić jednemu wykonawcy.

II. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO-UŻYTKOWE.

Szczegółowy opis wymagań minimalnych dla urządzeń i systemów teleinformatycznych przewidzianych w niniejszym postępowaniu dla poszczególnych części zamówienia przedstawiono w zestawieniu tabelarycznym.

Część I - Dostawa szafy teleinformatycznej Rack 42U z wyposażeniem oraz dodatkowymi akcesoriami – 1 szt.

Minimalne wymagania dla szafy teleinformatycznej Rack 42U z wyposażeniem - 1 szt.	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	Szafa teleinformatyczna W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanej szafy.
Zastosowanie	Do zabudowy pasywnym i aktywnym sprzętem serwerowym i sieciowym
Cechy fizyczne	Obciążalność min. 1000 kg Możliwość montażu urządzeń o sumarycznej wysokości 42U Wymiary szafy: min. 800mmx1000mmx2055mm (szerokość/głębokość/wysokość) Wyposażona w 4 stopki z regulacją wysokości
Konstrukcja	Grubość materiału: Rama, góra, dół, przednie drzwi, tylne drzwi, boczne drzwi: 1,2 mm Szyny poziome: 1,5 mm Szyny pionowe: 2,0 mm
Drzwi	Drzwi przednie przeszklone (z wklejoną szybą hartowaną) z wentylowanymi bokami, wyposażone w zamek. Drzwi tylne stalowe perforowane, wentylowane, wyposażone w zamek. Zdejmowane panele boczne.
Stopień ochrony	Co najmniej IP20
Wyposażenie	1. Panel 4 wentylatorów z termostatem, wysokość montażowa Rack 1U. 2. Półka rackowa uniwersalna, wysokość montażowa max 1U, głębokość min. 270mm, mocowanie czteropunktowe doczołowe – min. 1 sztuka 3. Panel zaślepiający wykonany ze stali, do zaślepienia pustych przestrzeni pomiędzy urządzeniami dostarczonymi i zamontowanymi w szafie Rack w ramach realizacji niniejszego postępowania - Zamawiający wymaga aby nad urządzeniem (pod urządzeniem) znalazł się jeden panel, wysokość montażowa panela max 1U, montaż doczołowy

	czteropunktowy. 4. Poziomy organizer kabli, wysokość montażowa max 1U, montaż doczołowy do szyn Rack – min. 1 sztuka 5. Szafa wyposażona w zestaw śrub, podkładek, koszyków przystosowanych do montażu wewnątrz szafy pozwalający na montaż wszystkich akcesoriów takich jak: patch panele, listwy zasilające, półki do pionowych szyn w każdej szafie Rack w ilości wymaganej przez zamontowane urządzenia. 6. 2x Patch panel UTP 19" 24x RJ45 kat.6, tacka złącza KRONE. 7. Zestaw narzędzi do budowy sieci LAN w tym: a) Narzędzie uderzeniowe LSA, zwane również nożem terminującym do złącz Krone IDC 110 oraz nożem krosowniczym. b) Ściągacz izolacji UTP, FTP, SFTP, TEL. c) Zaciskacz konektorów modularnych: 8p (RJ-45 - 8P8C). d) Tester kabli RJ-45, RJ-12, RJ-11. e) Tester okablowania z identyfikatorem par kabli RJ-45, RJ-12, RJ-11.
Gwarancja producenta	Min. 24 miesiące

Usługi w zakresie dostarczenia i montażu szafy teleinformatycznej.	
Parametr	**Charakterystyka (wymagania minimalne)**
Usługi	Celem prac jest montaż szafy teleinformatycznej we wskazanym przez Zamawiającego pomieszczeniu celem przygotowania jej do instalacji dostarczonego w ramach projektu sprzętu informatycznego. Zamawiający umożliwi Wykonawcy dostęp do pomieszczenia w ustalonym wcześniej terminie. Dostęp do pomieszczenia będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia instalacji. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.
Montaż	Zamawiający wymaga zainstalowania szafy teletechnicznej w pomieszczeniu serwerowni co najmniej w następującym zakresie: 1. Wniesienie, ustawienie i fizyczny montaż szafy Rack w pomieszczeniu wskazanym przez Zamawiającego. 2. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji szafy.

Część II - Dostawa serwerów wraz z oprogramowaniem z usługą wdrożenia – 3 szt..

Załącznik nr 3 do SWZ

Minimalne wymagania dla serwera (typ 1)	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	Serwer. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera.
Funkcjonalność obudowy	1. Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. 2. Wyposażona 4 porty USB z czego nie mniej niż 1 port USB 3.0, 2 porty VGA z czego jeden port video na panelu przednim.
Procesory	Zainstalowane dwa procesory min. 8-rdzeniowe, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 139 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. **Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty raport z testu wydajności SPECrate®2017_int_base opublikowany na stronie www.spec.org dla oferowanego modelu serwera z oferowanym modelem procesora, w konfiguracji dwuprocesorowej.**
Funkcjonalność płyty głównej	Płyta główna wyposażona w minimum: 1. 16 slotów (gniazd) pamięci RAM przeznaczonych do instalacji pamięci RAM. 2. 2 sloty PCIe x16 generacji 4 3. Moduł TPM 2.0
Pamięć RAM	Minimum 128GB z możliwością rozbudowy do 1TB pamięci RAM
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Interfejsy sieciowe/FC/SAS	1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT 2. Dodatkowa dwuportowa karta sieciowa 10GbE SFP+
Kable/wkładki	2x kompatybilny kabel DAC SFP+/SFP+ 10GbE min. 3m
Dyski twarde	1. Zainstalowane 3 dyski SSD SAS o pojemności min. 960GB, 12Gb, 2,5“ Hot-Plug. 2. Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1.
Zasilanie	Zasilacze Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Możliwość dynamicznego włączania i wyłączania portów USB na

	obudowie - bez potrzeby restartu serwera 6. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. możliwość podmontowania zdalnych wirtualnych napędów; 5. wirtualną konsolę z dostępem do myszy, klawiatury; 6. wsparcie dla IPv6; 7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 10. integracja z Active Directory; 11. możliwość obsługi przez dwóch administratorów jednocześnie; 12. wsparcie dla dynamic DNS; 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; 14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera; 15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Normy, certyfikaty i standardy	1. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE. 2. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022.
Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	1. Serwer w ramach wymagań podstawowych musi być objęty serwisem gwarancyjnym producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 3 lata (36 miesięcy), z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. 2. Wymagana jest możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego. Zamawiający po wyborze wykonawcy (przed podpisaniem umowy) będzie żądał złożenia oświadczenia od podmiotu realizującego serwis lub od producenta sprzętu potwierdzającego spełnienie w/w wymagania dla realizowanej dostawy. 4. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa

	w pkt 1 musi odpowiadać okresowi udzielonej gwarancji na sprzęt. 5. Zaoferowane serwery muszą mieć możliwość rozszerzenia gwarancji przez producenta do 5 lat. 6. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. 7. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
System operacyjny/ System wirtualizacji	Serwerowy system operacyjny Microsoft Windows Serwer 2022 lub równoważny. Warunki równoważności: System operacyjny 64-bit. Za rozwiązanie równoważne uznaje się takie, które posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji (bez jakichkolwiek emulatorów, implementacji lub programów towarzyszących), zapewniające: 1. Polską wersję językową. 2. Możliwość instalacji i poprawnego działania aplikacji wykorzystywanych przez Zamawiającego, oraz poprawnej obsługi powszechnie używanych urządzeń peryferyjnych (drukarek, skanerów, kser), 3. Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. 4. Licencje serwerowego systemu operacyjnego muszą uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym. 5. Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. 6. Jeśli do legalnego korzystania z oprogramowania serwera (w zgodzie z licencją) jest wymagana licencja dostępowa (Client Access License) zapewniająca użytkownikowi prawo do korzystania z usług serwera, to należy przewidzieć dostawę sumarycznie 35 licencji dostępowych na użytkownika współpracujących z oferowanym systemem operacyjnym. 7. Jeśli do legalnego korzystania z pulpitu zdalnego serwera (w zgodzie z licencją) jest wymagana licencja RDS (Remote Desktop Services) zapewniająca użytkownikowi prawo do korzystania z usług pulpitu zdalnego, to należy przewidzieć dostawę sumarycznie 35 licencji na użytkownika współpracujących z oferowanym systemem operacyjnym. 8. System musi być nowy (nie aktywowany wcześniej na innym urządzeniu). 9. System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowa-

	nym urządzeniu komputerowym. 10. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. 11. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta. Warunki równoważności: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego (domeną Active Directory pracującą w oparciu o system Windows Server 2019) musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server. 5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. 7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a) zarządzania użytkownikami, b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c) możliwości przydzielania praw dostępu do zasobów sieciowych, d) instalacji zdalnej oprogramowania z pakietów msi, e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 10 i 11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. 11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT)

	oraz Windows Admin Centre. 12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. 13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 15. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra. 16. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 17. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 18. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6. 19. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny. 20. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 21. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1. 22. System operacyjny musi posiadać obsługę certyfikatów w Active Directory. 23. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). Wymagania dla równoważnych licencji dostępowych dla urządzenia: • Licencja dostępowa dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu User Cal z wdrożoną rolą Active Directory. • Każda z licencji musi pozwalać na dostęp wielu użytkowników z jednego, licencjonowanego urządzenia do zasobów serwera. W przypadku zaproponowania przez Dostawcę oprogramowania równoważnego zobowiązuje się on do: • wdrożenia oprogramowania oraz przeprowadzenia certyfikowanych szkoleń dla użytkowników oferowanego rozwiązania w wymiarze co najmniej 40 godzin. • pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdro-

	żenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania

Minimalne wymagania dla serwera (typ 2)	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	Serwer. W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera.
Funkcjonalność obudowy	1. Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. 2. Wyposażona 4 porty USB z czego nie mniej niż 1 port USB 3.0, 2 porty VGA z czego jeden port video na panelu przednim.
Procesory	Zainstalowane dwa procesory min. 8-rdzeniowe, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 139 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. **Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty raport z testu wydajności SPECrate®2017_int_base opublikowany na stronie www.spec.org dla oferowanego modelu serwera z oferowanym modelem procesora, w konfiguracji dwuprocesorowej.**
Funkcjonalność płyty głównej	Płyta główna wyposażona w minimum: 1. 16 slotów (gniazd) pamięci RAM przeznaczonych do instalacji pamięci RAM. 2. 2 sloty PCIe x16 generacji 4 3. Moduł TPM 2.0
Pamięć RAM	Minimum 128GB z możliwością rozbudowy do 1TB pamięci RAM
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Interfejsy sieciowe/FC/SAS	1. min. 4 interfejsy sieciowe 1GbE w standardzie BaseT 2. min. 2 interfejsy sieciowe 10/25GbE SFP28
Kable/wkładki	2x Kabel, SFP+ do SFP+, 10GbE, dwuosiowy kabel miedziany podłączany bezpośrednio, min. 3 metry
Dyski twarde	1. Zainstalowane 3 dyski SSD SAS o pojemności min. 960GB, 12Gb, 2,5“ Hot-Plug. 2. Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1.
Zasilanie	Zasilacze Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

	4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie - bez potrzeby restartu serwera 6. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. możliwość podmontowania zdalnych wirtualnych napędów; 5. wirtualną konsolę z dostępem do myszy, klawiatury; 6. wsparcie dla IPv6; 7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 10. integracja z Active Directory; 11. możliwość obsługi przez dwóch administratorów jednocześnie; 12. wsparcie dla dynamic DNS; 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; 14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera; 15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Normy, certyfikaty i standardy	1. Oferowany sprzęt musi posiadać certyfikację oraz oznaczenie CE. 2. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022.
Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	1. Serwer w ramach wymagań podstawowych musi być objęty serwisem gwarancyjnym producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 3 lata (36 miesięcy), z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. 2. Wymagana jest możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. W przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wparciem technicznym) powodującej konieczność jego wymiany, uszkodzony dysk pozostaje u Zamawiającego. Zamawiający po wyborze wykonawcy (przed podpisaniem umowy) będzie żądał złożenia oświadczenia od podmiotu realizującego serwis

	lub od producenta sprzętu potwierdzającego spełnienie w/w wymagania dla realizowanej dostawy. 4. Okres zabezpieczenia serwisowego na dyski twarde, o którym mowa w pkt 1 musi odpowiadać okresowi udzielonej gwarancji na sprzęt. 5. Zaoferowane serwery muszą mieć możliwość rozszerzenia gwarancji przez producenta do 5 lat. 6. Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia. 7. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
System operacyjny/System wirtualizacji	Serwerowy system operacyjny Microsoft Windows Serwer 2022 lub równoważny. Warunki równoważności: System operacyjny 64-bit. Za rozwiązanie równoważne uznaje się takie, które posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji (bez jakichkolwiek emulatorów, implementacji lub programów towarzyszących), zapewniające: 1. Polską wersję językową. 2. Możliwość instalacji i poprawnego działania aplikacji wykorzystywanych przez Zamawiającego, oraz poprawnej obsługi powszechnie używanych urządzeń peryferyjnych (drukarek, skanerów, kser), 3. Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. 4. Licencje serwerowego systemu operacyjnego muszą uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym. 5. Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. 6. System musi być nowy (nie aktywowany wcześniej na innym urządzeniu). 7. System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowanym urządzeniu komputerowym. 8. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. 9. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta.

	Warunki równoważności: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego (domeną Active Directory pracującą w oparciu o system Windows Server 2019) musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server. 5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji. 7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a) zarządzania użytkownikami, b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową, c) możliwości przydzielania praw dostępu do zasobów sieciowych, d) instalacji zdalnej oprogramowania z pakietów msi, e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 10 i 11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. 11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre. 12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. 13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 15. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra.

	16. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 17. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 18. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6. 19. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny. 20. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 21. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1. 22. System operacyjny musi posiadać obsługę certyfikatów w Active Directory. 23. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). W przypadku zaproponowania przez Dostawcę oprogramowania równoważnego zobowiązuje się on do: • wdrożenia oprogramowania oraz przeprowadzenia certyfikowanych szkoleń dla użytkowników oferowanego rozwiązania w wymiarze co najmniej 40 godzin. • pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania

Minimalne wymagania dla serwera backupu – 1 szt.	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego serwera backupu.
Obudowa	Rack o wysokości max. 2U wraz z kompletem szyn teleskopowych wyposażona we wskaźniki diodowe określające następujące statusy: HDD 1-8, stan, LAN, Power, USB
Pamięć	Min. 4GB RAM z możliwością rozbudowy do 16GB 512 MB Flash 32TB pamięci dyskowej (8x4TB) wyposażonej w min. 128MB pamięci podręcznej dla każdego dysku
Ilość obsługiwanych dys-	8 dysków 2.5"/3.5" SATA Hot Swap o maksymalnej pojemności 18TB każdy

ków	
Interfejsy sieciowe	2x 2.5 Gbit (2,5G/1G/100M) lub 4x 1GBit, 2x 10 GbE SFP+
Porty	4x USB 3.2 Gen 1, 1x PCIe Gen 2x2
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 5+Spare, 6, 6+Spare, 10, 10+Spare, 50/60.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID.
Szyfrowanie	Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Mechanizm szyfrowania z akceleracją sprzętową.
Obsługiwane protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Serwer VPN
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Język GUI	Polski
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ oraz exFAT
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	Zasilacze redundatne o mocy min. 250W (x2)
Wentylatory	Minimum 2, o wymiarach co najmniej 70mm
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS
Gwarancja producenta Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	Serwer backupowy w ramach wymagań podstawowych musi być objęty serwisem gwarancyjnym producenta lub serwisem gwarancyjnym autoryzowanego partnera serwisowego producenta w miejscu instalacji sprzętu (dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu) przez min. 36 miesięcy, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.
Wymagania minimalne dla licencji na oprogramowanie do realizacji kopii zapasowych	1. W ramach licencji wieczystej (bezterminowej) oprogramowanie musi zapewnić realizację kopii zapasowych z 3 (trzech) serwerów fizycznych i 2 (dwóch) maszyn wirtualnych. 2. Wykonawca zapewnieni wsparcie techniczne (support producenta) dla dostarczonego oprogramowania przez okres 1 roku (12 miesięcy) lecz nie dłużej niż do 30.09.2023 r. 3. Oprogramowanie musi współpracować z infrastrukturą Microsoft

	Hyper-V 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. 4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger oraz pojedynczymi hostami. 5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych i stacji roboczych opartych o Windows **Całkowite koszty posiadania** 1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. 2. Oprogramowanie musi tworzyć „samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków 3. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) 4. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. 5. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. 6. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych takiej puli. 7. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania 8. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. 9. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. 10. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji. 11. Oprogramowanie musi posiadać mechanizmy chroniące przed utra-

	tą hasła szyfrowania. 12. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. **Wymagania RPO** 1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. 2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych. 4. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru. 5. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora. 6. Oprogramowanie musi posiadać wsparcie dla NDMP 7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 8. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. 9. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. 10. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2019 z systemem pliku ReFS jako repozytorium backupu. 11. Repozytoria oparte o XFS muszą pozwalać na zmienność danych przez określoną ilość czasu (tzw Immutability) 12. Oprogramowanie musi mieć możliwość kopiowania backupów. **Wymagania RTO** 1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowiska Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. 2. Oprogramowanie musi pozwalać na migrację on-line tak uruchomio-

	nych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami. 3. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. 4. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. 5. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, PowerShell Direct dla platformy Hyper-V. 6. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: a. Windows: NTFS, FAT, FAT32, ReFS 7. Oprogramowanie musi wspierać przywracanie plików z partycji Windows Storage Spaces. 8. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 9. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. 10. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. 11. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2019 i nowszych 12. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska. 13. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego. **Ograniczenie ryzyka** 1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. 2. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem 3. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection

	Engine oraz ESET NOD32. 4. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. **Monitoring** 1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich 2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2019 i 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. 3. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter. 4. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. 5. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel. 6. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk. 7. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. 8. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. 9. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). 10. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. 11. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego. 12. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta. 13. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 14. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

Raportowanie

1. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na Microsoft Hyper-V 2019 i 2022
2. System musi wspierać wiele instancji Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
3. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach Hyper-V.
4. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
5. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
6. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
7. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
8. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
9. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
10. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
11. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
12. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
13. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
14. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

Agent

1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3. Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików:
   - NTFS, FAT, FAT32, ReFS.

4. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
5. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
6. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
7. Rozwiązanie musi wspierać backup podłączonych dysków USB
8. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
9. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
   - Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny
   - Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire
   - Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
   - Zcentralizowanym repozytorium danych
10. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
11. Rozwiązanie musi wspierać kontrolę pasma sieciowego
12. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
13. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
14. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
15. Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
16. Rozwiązanie musi wspierać technologię BitLocker
17. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
18. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
    - Microsoft Active Directory 2003 i nowszych
    - Microsoft SQL 2019 i nowszych
19. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
20. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
21. Rozwiązanie musi wspierać szyfrowanie
22. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (ca-

	che) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne 23. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego 24. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej 25. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.	
Parametr	**Charakterystyka (wymagania minimalne)**
Usługi	Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji projektu, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia i uruchomienia nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. Zamawiający wymaga sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.
Montaż i fizyczne uruchomienie systemu	Zamawiający wymaga zainstalowania wskazanego, dostarczonego rozwiązania w pomieszczeniu serwerowni, lub w innych wskazanych miejscach co najmniej w następującym zakresie: 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń: serwery (typ 1 i 2), serwer backupowy. 2. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 3. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 5. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 6. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami zamontowanymi w szafie Rack, w celu zapewnienia komuni-

	kacji - Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane (min. kat. 6 UTP) lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 7. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające do szafy Rack). 8. Po wykonaniu instalacji przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzeń.
Instalacja i konfiguracja serwerów, instalacja systemu operacyjnego serwerów	Fizyczna instalacja dwóch serwerów w szafie Rack. Konfiguracja odpowiedniego poziomu RAID wskazana przez Zamawiającego. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Instalacja niezbędnych aktualizacji oraz poprawek związanych z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
Uruchomienie środowiska wirtualizacyjnego	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w następującym zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego (jeżeli jest wymagana) 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego - aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach. 4. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 5. Konfiguracja serwerów wirtualizacyjnych. 6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 7. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 8. Przygotowania koncepcji i wykonania wirtualizacji do 1 wirtualnej maszyny. 9. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 10. Konfiguracja replikacji maszyn wirtualnych: a. Konfiguracja mechanizmów HA - w przypadku awarii węzła wirtualna maszyna, które jest na nim uruchomiona musi zostać przeniesiona na sprawny węzeł klastra bez ingerencji użytkownika. b. Konfiguracja mechanizmów przenoszenia uruchomionej wirtualnej maszyny pomiędzy węzłami bez utraty dostępu do zasobów wirtualnej maszyny.

	c. Konfiguracja mechanizmów ochrony wirtualnej maszyny przed awarią fizycznego serwera. 11. Weryfikacja działania replikacji maszyn wirtualnych.
Uruchomienie i konfiguracja systemu zarządzania kopiami zapasowymi	Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych (serwer backupowy NAS) oraz aktywacja wymaganych licencji. Wymagana będzie konfiguracja zadań wykonywania kopii zapasowych wirtualnych maszyn według poniższych wymagań: 1. Kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; 2. Kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; 3. Kopie maszyn wirtualnych muszą być replikowane na wskazany przez Zamawiającego zasób dyskowy; 4. Kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; 5. Kopie zapasowe muszą (jeżeli jest taka funkcjonalność) być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; 6. Musi istnieć możliwość odtworzenia: całej wirtualnej maszyny, dysku wirtualnej maszyny, pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); Oprogramowanie musi umożliwiać: 1. Replikację maszyn wirtualnych w oparciu o obrazy. 2. Syntetyczną pełną kopię zapasową - tworzenie kopii zapasowych forever-incremental. 3. Tworzenie harmonogramów kopii zapasowych bezpośrednio z UI. 4. Weryfikacja kopii zapasowej pod kątem infekcji i złośliwego oprogramowania przed przywróceniem do środowiska produkcyjnego. 5. Konfiguracja powiadomień o wykonaniu kopii zapasowej (e-mail). Rozwiązanie zostanie poddane testowaniu poprzez: 1. Uruchomienie testowych zadań backupu. 2. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień e-mail. 3. Uruchomienie testowych zadań odtworzenia danych.
Wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.

Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej)

Część III - Dostawa, konfiguracja oraz uruchomienie urządzenia UTM – 1 kpl.

Wymagania minimalne dla urządzenia UTM – szt. 1	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia (rozwiązania).
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System musi wspierać IPv4 oraz IPv6 w zakresie: ▪ Firewall. ▪ Ochrony w warstwie aplikacji. ▪ Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: ▪ 5 portami Gigabit Ethernet RJ-45. ▪ 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.
Parametry wydajnościo-	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.

we	2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 300 Mbps. 5. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Zamawiający dopuszcza aby były one zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
Połączenia	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W

VPN	zakresie tej funkcji musi zapewniać: ▪ Wsparcie dla IKE v1 oraz v2. ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). ▪ Obsługa protokołu Diffie-Hellman grup 19 i 20. ▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. ▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: ▪ Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. ▪ Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: ▪ Routingu statycznego. ▪ Policy Based Routingu. ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

	3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 5. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola www	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL. 5. Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych

	treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: ▪ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. ▪ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. ▪ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 6. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie bezpośrednio na urządzeniu w nastepmnej kolejności do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach dostawy musi zostać zapewniony (dostarczony) komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważ-

	niające do składowania logów. 3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 5. Musi istnieć możliwość logowania do serwera SYSLOG.
Serwisy i licencje	W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów Powinny one obejmować: 1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen 2. Licencja na usługę realizowaną w chmurze umożliwiająca logowanie i raportowanie z czasem retencji logów.
Warunki gwarancyjno-serwisowe, wsparcie techniczne producenta	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 2 lat (24 miesięcy), polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wymagania ogólne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.	
Parametr	**Charakterystyka (wymagania minimalne)**
Usługi	Celem prac jest przygotowanie środowiska teleinformatycznego, na po-

	trzeby realizacji projektu, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia i uruchomienia nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. Zamawiający wymaga sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.
Montaż i fizyczne uruchomienie systemu	Zamawiający wymaga zainstalowania wskazanego, dostarczonego rozwiązania w pomieszczeniu serwerowni, lub w innych wskazanych miejscach co najmniej w następującym zakresie: 3. Wniesienie, ustawienie i fizyczny montaż urządzenia UTM. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonym urządzeniem zamontowanym w szafie Rack, w celu zapewnienia komunikacji - Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane (min. kat. 6 UTP) lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzenia do sieci elektrycznej (np.: listwy zasilające do szafy Rack). 10. Po wykonaniu instalacji przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzenia.
Konfiguracja elementów bezpieczeństwa sieciowego	1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)

	4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu gminy 5. Konfiguracja dostarczonego systemu Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT; c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną serwery; d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS, SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej z uwierzytelnieniem w oparciu o usługę katalogową. 9. Uruchomienie i skonfigurowanie instancji systemów bezpieczeństwa dla skonfigurowanych sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z zamawiającym. 10. W instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zapora ogniowa klasy Statless Inspection b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogra-

	mowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma 11. Konfiguracja logowania i raportowania. 12. Konfiguracja logowania i raportowania do alternatywnego serwera SYSLOG uruchomionego na serwerze NAS (instalacja i konfiguracja serwera SYSLOG spoczywa na Wykonawcy). Jeśli dla zapewnienia tej funkcjonalności wymagane są jakiekolwiek licencje - ich dostarczenie spoczywa na Wykonawcy.
Wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.
Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej)

Część IV - Dostawa, konfiguracja, uruchomienie skanera dokumentów oraz wdrożenie oprogramowania do skanowania – 1 kpl.

Wymagania minimalne dla skanera dokumentów – 1 szt.	
Parametr	**Charakterystyka (wymagania minimalne)**
Typ	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia (rozwiązania).
Typ skanera	Skaner z automatycznym podajnikiem dokumentów ADF
Tryb skanowania	Skanowanie dwustronne jednoprzebiegowe (duplex) w trybach: kolor / skala szarości / monochromatyczny
Przeznaczenie urządzenia	Skanowanie dokumentów o różnych formatach i gramaturach bez konieczności ich wcześniejszej segregacji
Format ska-	A4, A5,A6,A7,B4,B5,B6,B7 i mniejsze

nowanych dokumentów	
Ilość układów optycznych i tryb	2 Możliwość skanowania w trybie duplex z podajnika ADF
Element światłoczuły dla ADF	CIS
Prędkość skanowania dla 300 dpi tryb czarno-biały, skala szarości, kolor	minimum 50 arkuszy/min, minimum 100 obrazów/min
Rozdzielczość optyczna	600 x 600 dpi
Zakres rozdzielczości wyjściowej	75 - 1200 dpi
Panel kontrolny skanera	4 liniowy – kolorowy LCD z możliwością predefiniowania profili skanowania, ich indywidualnego opisu i uruchamiania z poziomu skanera z polskim interfejsem wielkości minimum 1,5 cala
Automatyczny podajnik dokumentów	Urządzenie musi umożliwiać skanowanie kopert A4 i mniejszych przy użyciu ADF za pomocą prostej ścieżki prowadzenia papieru z interaktywnym przywracaniem pobrania wielu arkuszy
Wsparcie dla sterowników	TWAIN oraz ISIS
Poprawa jakości skanowanych dokumentów i funkcjonalności dla sterowników TWAIN/ISIS	Automatyczne rozpoznawanie wielkości i rozmiaru dokumentu, usuwanie kolorów; skanowanie dwustrumieniowe kolor i czarno-biały za jednym przebiegiem; interaktywna regulacja koloru, regulacja jasności i kontrastu, automatyczna rotacja dokumentu, automatyczne wykrywanie koloru, inteligentne wygładzanie koloru tła, inteligentne wypełnienie krawędzi obrazu, scalanie obrazów, wykrywanie pustych stron na podstawie procentowej zawartości oraz rozmiarze pliku, filtrowanie smug, filtr ostrości, fizyczne układanie dokumentów do krawędzi (likwidacja przekosu)
Format plik wyjściowego	Jedno i wielostronicowy TIFF, JPEG, RTF, BMP, PDF, PDF z możliwością wyszukiwania do j. polskiego, TXT, PNG, CSV, pliki Word i Excel
Format pliku indeksowego	Możliwość generowania pliku xml lub csv - zawierającego informację na temat liczby zeskanowanych stron, nazwy pliku oraz wartości odczytanego kodu kreskowego, np.: Interleaved 2 of 5, Code 3 of 9, Code 128, Codabar, UPC-A, UPC-E, EAN-13, EAN-8, PDF417, Data Matrix, QR code
Interfejsy komunikacyjne	USB 3.0 lub szybszy, Ethernet 10/100 Mbps wbudowany w urządzenie (Zamawiający nie dopuszcza różnego rodzaju zewnętrznych kart rozszerzeń) z obsługą standardu https
Możliwe obciążenie	do 6 000 skanów

dzienne	
Maksymalne natężenie dźwięku podczas skanowania	50 dB
Maksymalna wspierana przez skaner długość dokumentu	3 000 mm
Zakres gramatury skanowanych dokumentów dla ADF	od 28 g/m2 do 430 g/m2
Ochrona dokumentów przed zgnieceniem w osobnym czujniku	tak – regulacja czułości z poziomu sterownika TWAIN oraz ISIS
Czujnik podwójnych pobrań dokumentów	tak
Wsparcie producenta dla skanowania kart (wytłaczane twarde, karty plastikowe, dowody osobiste)	tak
Zarządzanie i monitoring (cechy i funkcjonalność)	Skaner musi współpracować z aplikacją do zdalnej aktualizacji sterowników oraz umożliwiać zdalną konfigurację profili skanowania z poziomu serwera, Generowanie raportów dotyczących stanu zużycia skanera i części eksploatacyjnych, generowanie monitów np. dotyczących potrzeby przeprowadzenia konserwacji skanera
Zastosowany rodzaj pamięci	NVRAM i SDRAM
Bezpieczeństwo skanowanych dokumentów	Dane skanowanych obrazów przechowywane są w pamięci ulotnej (SDRAM) – po wyłączeniu skanera dane są automatycznie usuwane
Wspierane systemy ope-	Windows 10 Pro (wersja 64-bitowa), Windows SERVER 2022 Standard (wersja 64-bitowa), Windows SERVER 2019 Standard (wersja 64-

racyjne dla sterowników TWAIN oraz ISIS	bitowa)
Zasilanie	100 - 240 V AC, 50 - 60 Hz
Pobór mocy	w trybie uśpienia do 5 W, tryb pracy do 36 W
Waga	do 3,5 kg
Deklaracja zgodności	Urządzenie musi posiadać oznakowanie CE
Ochrona środowiska	Oferowany sprzęt musi spełniać wymogi normy Energy Star tj. posiadać certyfikat lub spełniać kryteria efektywności energetycznej co najmniej równoważne z koniecznymi do uzyskania takiego oznaczenia. Zgodność z normą EPEAT
Oświadczenia	Oświadczenie producenta, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta przejmie na siebie wszelkie zobowiązania związane z serwisem urządzeń. Oświadczenie potwierdzające pochodzenie oferowanego sprzętu z oficjalnego polskiego kanału dystrybucji, podpisane przez producenta bądź autoryzowanego partnera na terenie Polski. **Dokumenty potwierdzające spełnienie ww. należy dołączyć do oferty**
Gwarancja	36 miesięcy z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.
Oprogramowanie do skanowania dokumentów wraz z licencjami	Oprogramowanie do przetwarzania wsadowego dokumentów, indeksowania oraz automatycznego OCR. Automatyzuje zamianę dokumentów z postaci papierowej oraz ich wprowadzanie do systemu obiegu dokumentów w zakresie: a) wspomagania skanowania, b) opisu pełno tekstowego OCR, odczytu OMR c) automatycznego wprowadzania do systemu obiegu dokumentów; 1. Oprogramowanie zapewnia obsługę wsadów dokumentów, w której dokumenty separowane są kodami kreskowymi (np. drukowanymi na stanowisku przyjmowania dokumentów), kodami typu patch, pustą kartką, ilością skanów oraz separacją po zmianie wartości w polu OCR (indeksie); 2. Oprogramowanie zapewnia możliwość automatycznego OCR i rozpoznawania znaków OMR skanowanych pism bez limitu skanowanych/procesowanych dokumentów; 3. Przez skanowanie rozumie się możliwość odczytania dokumentów z dysku twardego (przetwarzania dokumentów z wybranego folderu) lub skanowania ze skanera dokumentowego; 4. Oprogramowanie na zeskanowanych dokumentach pozwala na rozpoznawanie i indeksowanie co najmniej 22 typów kodów kreskowych takich typów jak Aztec, Codebar, Code 39, Code 93, Code 128, Data Matrix, EAN, Interleaved 2 of 5, PDF 417, Post Net, QR, Code 2 of 5, UPC-A, UPC-E;

	5. Oprogramowanie na zeskanowanych dokumentach daje możliwość filtrowania rozpoznawanych kodów do długości, formatów jakie mają spełniać skanowane kody oraz możliwość kontrolowania sumy kontrolnej kodów dla kodów kreskowych obsługujących sumy kontrolne (typy kodów które obsługują sumy kontrolne zapisywane na ostatnich pozycjach to Codebar, Code 39, Interleaved 2 of 5); 6. Oprogramowanie zapewnia rozpoznanie kodu kreskowego na pierwszej stronie również na rewersie dokumentu. W momencie braku takowego na pierwszej stronie odczyt z drugiej lub trzeciej strony będzie zapewniony; 7. Oprogramowanie pozwala na zaprogramowanie odpowiednich pól indeksowych, które muszą być rozpoznane w sposób automatyczny oraz umożliwić wprowadzenie wartości indeksu ręcznie bądź za pomocą metody point&click oraz drag&drop. Każde pole indeksowe musi pozwalać na wybór języka OCR; 8. Oprogramowanie pozwala na separację zeskanowanych dokumentów na podstawie rozpoznanych i przefiltrowanych kodów obcych zarówno z pierwszej jak i drugiej strony dokumentu wiodącego. W momencie braku takowego na pierwszej stronie odczyt z drugiej lub trzeciej strony będzie zapewniony; 9. Oprogramowanie pozwala na separację zeskanowanych dokumentów na podstawie pustych stron z możliwością konfiguracji takiego algorytmu rozpoznawania pustych; 10. Oprogramowanie pozwala na separację zeskanowanych dokumentów na podstawie stałej zadeklarowanej ilości stron na dokument; Strona 7 z 12 2.43 11. Oprogramowanie daje możliwość zeskanowania jednej strony lub całej ilości dokumentów; 12. Oprogramowanie pozwala na zapis plików na serwerach FTP, SFTP. 13. Oprogramowanie daje możliwość wyboru podajnika skanera (ręczny lub automatyczny); 14. Oprogramowanie daje możliwość wyboru trybu skanowania (jednostronny/dwustronny); 15. Oprogramowanie daje możliwość wyboru rozmiaru papieru do skanowania oraz wyboru orientacji skanowania (pozioma, pionowa); 16. Oprogramowanie daje możliwość dodatkowej automatycznej rotacji skanowanych dokumentów o podstawowe kąty: 90, 180, 270 stopni. Możliwość definiowania obrotu na każdą stronę oddzielnie; 17. Oprogramowanie pozwala na doskanowanie dokumentu do całej przetwarzanej grupy; 18. Oprogramowanie daje możliwość podglądu na listę zeskanowanych i porozdzielanych dokumentów. Podział następuje według wcześniej wspomnianych kryteriów. Widok podziału rozumie się poprzez możliwość przejrzenia wszystkich zeskanowanych stron pogrupowane w procesie separacji na dokumenty; 19. Oprogramowanie daje możliwość doskanowania strony w wybranym miejscu, przykładowo dla wybranego dokumentu z całego widoku można doskanować stronę, ponieważ została pominięta.

	20. Oprogramowanie daje możliwość wymiany jednej strony z całego odseparowanego dokumentu, przykładowo 5 strona z wybranego dokumentu posiada wadę skanowania i należy ją podmienić skanując ją ponownie; 21. Oprogramowanie daje możliwość przeskanowania całego wybranego dokumentu, tak aby w przypadku stwierdzenia złego zeskanowania konkretnego dokumentu nie wymagałoby to skanowania całej grupy dokumentów a tylko wymiany tego jednego wadliwego; 22. Oprogramowanie daje możliwość łatwej modyfikacji dokumentów a więc przenoszenia stron i dokumentów w obrębie całej grupy zeskanowanych dokumentów; 23. Oprogramowanie daje możliwość automatycznego przełączania zaprogramowanych zadań lub ustawień skanera za pomocą kodów typu patch umieszczonego pomiędzy skanowanymi dokumentami; 24. Umożliwia cofanie wykonywanych operacji; 25. Oprogramowanie daje możliwość przywrócenia pracy nad zeskanowaną grupą dokumentów po zaniku napięcia na stacji skanującej. Aplikacja w tle przechowuje dane na dysku twardym, aby możliwe było ewentualne odtworzenie, po zaniku napięcia na stacji roboczej, zeskanowanych dokumentów, tak aby nie powtarzać procesu skanowania; 26. Oprogramowanie daje możliwość exportu przetworzonych dokumentów do wskazanego folderu. Exportowane dokumenty powinny mieć możliwość konfiguracji nazewnictwa wykorzystując przy tworzeniu dynamicznych nazw wcześniej rozpoznanych kodów, stałej znakowej, nazwy stacji wykonującej skanowanie, nazwy użytkownika, daty i czasu wykonania operacji. Eksport umożliwiać powinien wyeksportowanie dokumentów w formatach: PDF, PDF-A, PDF-MRC, PDF-BookMark mode, TIFF, JPG; Strona 8 z 12 2.43 27. Dynamiczny podgląd dokumentów podczas skanowania; 28. Umożliwia przetwarzanie dokumentów z folderu takich typów jak TIFF, BMP, JPEG, PDF; 29. Umożliwia dla eksportowanych dokumentów PDF ich przeszukiwanie (wyszukiwanie tekstu w dokumentach PDF) oraz zapewnia zabezpieczenie takiego pliku hasłem; 30. Umożliwia eksport wytworzonych dokumentów do programu Microsoft Sharepoint z automatycznie rozpoznanymi polami indeksowymi i ich publikacją w bibliotekach; 31. Umożliwia eksportowanie dokumentów w tle tak aby możliwe było w tym czasie kolejne skanowanie dokumentów; 32. Umożliwia walidację rozpoznawanych pól przy użyciu sterowników ODBC które wyszukiwałyby w takiej bazie danych sterownika ODBC rozpoznanego tekstu; 33. Umożliwia tworzenie indywidualnego interfejsu użytkownika dla każdej z zalogowanych osób; 34. Oprogramowanie posiada polski interfejs użytkownika oraz pozwala na wybór języka OCR przy indeksowaniu dla każdego z uprzednio definiowanych pól oraz w trybie pełno tekstowym;

	35. Uwierzytelnienie dla pracowników za pomocą loginu domenowego oraz Active Directory; 36. Oprogramowanie, musi posiadać pełną kompatybilność z systemem EZD PUW;

III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI

1. **Pozostałe wymagania stawiane Wykonawcom**
   Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania. Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych:
   a) koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia; (urządzeń) Zamawiającego przed ich zniszczeniem w trakcie wykonywania prac,
   b) koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego;
   c) koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac;
   d) koszty testów, prób, badań, odbiorów technicznych – jeśli są wymagane.

2. **Stosowanie rozwiązań z zakresu interoperacyjności**
   Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:
   a) zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
   b) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
   c) zapewnienia bezpieczeństwa plików;
   d) dbałość o aktualizację oprogramowania.

   Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).
   Konieczność zapewnienia tej funkcjonalności wynika z:
   a) §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej)
   b) Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

   <u>Wdrożone rozwiązania powinny spełniać wymagania przywołanych aktów prawnych oraz standardów rynkowych.</u>

3. **Dokumenty odbioru końcowego**
   a) Protokół odbioru końcowego
   b) Protokoły z pomiarów i testów - jeśli dotyczy

c) Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta.

Wykonawca na etapie realizacji zamówienia dostarczy w terminie 7 dni od dnia podpisania umowy z Zamawiającym certyfikaty i deklaracje a w szczególności deklarację zgodności CE, certyfikat potwierdzający spełnienie normy Energy Star 5.x lub nowszej, Certyfikat ISO 9001:2000 oraz Certyfikat ISO 14001 dla producenta sprzętu, potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.