



SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zamówienia: Projekt Cyberbezpieczny Samorząd - Zakup i dostawa sprzętu wraz z oprogramowaniem dla Gminy Kępno - Cyberbezpieczna Gmina Kępno

Numer referencyjny: WR.271.6.2025

Opis przedmiotu zamówienia

1. Zasilanie awaryjne :

A) Agregat prądotwórczy - 1 szt.

Przedmiotem zamówienia jest dostawa fabrycznie nowego, stacjonarnego, trójfazowego agregatu prądotwórczego z silnikiem Diesla, zabudowanego w obudowie wyciszonej wraz z niezbędnym wyposażeniem i dokumentacją, w celu zapewnienia zasilania awaryjnego (lub podstawowego - zależnie od potrzeb Zamawiającego). Agregat dostarczony pod adres ul. Kościuszki 9, 63-600 Kępno, z uwzględnieniem następujących minimalnych wymagań technicznych i norm jakościowych:

Minimalne wymagania techniczne

Poniższa tabela przedstawia kluczowe parametry techniczne, które musi spełnić oferowany agregat. Wykonawca może zaoferować urządzenie o parametrach równych lub wyższych niż wskazane, pod warunkiem zachowania zgodności z opisem przedmiotu zamówienia i standardami jakościowymi.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Lp	Parametr / Wymaganie	Minimalny wymóg / Opis
1	Moc znamionowa (PRP)	30 kVA / 24 kW (min. 24 kW przy współczynniku mocy 0,8)
2	Moc maksymalna (LTP)	33 kVA / 26,4 kW
3	Współczynnik mocy ($\cos \phi$)	0,8
4	Napięcie znamionowe	400/230 V, 50 Hz, trójfazowe
5	Silnik	<ul style="list-style-type: none">- Typ: wysokoprężny (Diesel), 4-suwowy, chłodzony cieczą- Liczba cylindrów: 4 w rzędzie (lub równoważna konstrukcja zapewniająca parametry mocy wg wiersza 1–2)- Prędkość obrotowa: 1500 obr./min- Instalacja rozruchowa: 12 V (rozruch elektryczny)- Zużycie paliwa: nie większe niż ok. 5,2 l/h przy 75% obciążenia PRP (lub równoważne, gwarantujące niskie spalanie i emisje)
6	Prądnica	<ul style="list-style-type: none">- Bezszcotkowa, trójfazowa, klasy izolacji co najmniej H, klasa ochrony IP \geq 23 - Zakres regulacji napięcia: $\pm 1\%$ (AVR lub równoważne rozwiązanie elektroniczne)
7	Obudowa wyciszona (canopy)	<ul style="list-style-type: none">- Wykonana z blachy stalowej malowanej proszkowo- Zapewniająca tłumienie hałasu do poziomu maks. 62 dB(A) @7m (lub niższy) - Konstrukcja odporna na warunki atmosferyczne (uszczelnienia, wentylacja, izolacja akustyczna)
8	Zbiornik paliwa	<ul style="list-style-type: none">- Zintegrowany z ramą urządzenia, o pojemności min. 170 litrów (lub większej) - Wyposażony w korek spustowy i zewnętrzny wlew paliwa
9	Wymiary	Nie większe niż ok. 2100 x 870 x 1165 mm (dopuszcza się niewielkie różnice)
10	Masa (waga)	Około 800–900 kg (lub w zakresie zapewniającym stabilność i przenośność w tej klasie mocy)
11	Poziom głośności	Maksymalnie 62 dB(A) w odległości 7 m (lub niższy)
12	System sterowania / panel automatyki	<ul style="list-style-type: none">- Sterownik z funkcją SZR (AMF), pozwalający na automatyczny rozruch i zatrzymanie agregatu w razie zaniku / powrotu zasilania sieciowego- Wyświetlacz umożliwiający odczyt parametrów (napięcie, częstotliwość, prąd, stan paliwa itp.)- Możliwość lokalnego i zdalnego monitorowania pracy agregatu (np. przez sieć, GSM, Ethernet – w zależności od preferencji Zamawiającego)



Cyberbezpieczny Samorząd

13	Zgodność z normami i dyrektywami	- Oznakowanie CE - Dyrektywy maszynowe 2006/42/CE, EMC 2014/30/UE, niskonapięciowe 2014/35/UE - Poziom hałasu zgodny z 2000/14/EC (i późniejszymi zmianami) - Emisja spalin zgodna z obowiązującymi normami (np. 97/68/EC i późn. zm.) - Certyfikaty ISO 8528, EN 60034-1 lub równoważne
14	Wyłącznik główny	Przystosowany do pełnej mocy agregatu (np. 50 A lub dostosowany do mocy znamionowej)
15	Gniazda odbioru mocy	Co najmniej 1 gniazdo trójfazowe (63 A) + dodatkowe gniazdo jednofazowe (jeżeli wymagane przez Zamawiającego)
16	Dostawa	Dostawa w miejscu wyznaczonym przez Zamawiającego, z zapewnieniem wszystkich niezbędnych materiałów eksploatacyjnych i prób funkcjonalnych.
17	Gwarancja	Minimum 24 miesiące

3. Dodatkowe wymagania

1. Dokumentacja

a) Wykonawca dostarczy w języku polskim (lub wraz z tłumaczeniem na j. polski) kompletną dokumentację techniczną, w tym instrukcję obsługi i konserwacji oraz schematy elektryczne.

b) Dokumentacja musi zawierać m.in atesty potwierdzające spełnienie wymagań norm i dyrektyw określonych w tabeli.

2. Szkolenie

a) Wykonawca zobowiązuje się przeprowadzić krótkie szkolenie w zakresie obsługi, konserwacji i podstawowych czynności serwisowych agregatu (personel wyznaczony przez Zamawiającego).

3. Wykonanie i wykończenie

a) Wszystkie elementy powinny być fabrycznie nowe, wolne od wad materiałowych i konstrukcyjnych.

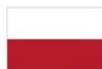
b) Agregat powinien być dostosowany do pracy w warunkach zewnętrznych przy temperaturach ujemnych i dodatnich (np. -15°C do +40°C, w zależności od warunków panujących u Zamawiającego).

c) Rama, obudowa oraz wszystkie elementy narażone na korozję muszą być zabezpieczone antykorozyjnie (farby i powłoki antykorozyjne, ocynk itp.).

4. Serwis i wsparcie



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

a) W trakcie okresu gwarancji Wykonawca ma obowiązek zapewnić serwis gwarancyjny.

B) UPS - 1 szt.

1. MOC min. - 3000VA/3000W
2. Obudowa - Rack
3. Topologia - Line-interactive
4. Kształt napięcia w trybie bateryjnym - Czyste napięcie sinusoidalne
5. Czas przełączania - do 4ms
6. Możliwość podłączenia zewnętrznych modułów bateryjnych
7. Czas podtrzymania dla obciążenia 1700 W co najmniej 30 min. z możliwością do wydłużenia czasu pracy do 3h
8. Czas ładowania akumulatorów - do 6 godzin dla całego systemu
9. Ilość gniazd wyjściowych - co najmniej 8
10. UPS musi posiadać wydzieloną grupę gniazd dla obciążeń kluczowych/krytycznych oraz dla pozostałych obciążeń .
11. Porty komunikacyjne:
USB
RS232
EPO
Dry contact
12. Komunikacja po protokole SNMP/HTTP - TAK
13. Oprogramowanie do zarządzania UPSem umożliwiające monitorowanie zużycia energii oraz z możliwością współpracy ze środowiskiem VMware ESXi 8.0 U2
14. Rozproszenie ciepła online (BTU/h) - do 125 BTU/h
15. Gwarancja - minimum 2 lata



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



2. Serwer

Serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none">Obudowa Rack o wysokości max 1U.Możliwość instalacji minimum 10 dysków 2.5".Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	<ul style="list-style-type: none">Płyta główna z możliwością zainstalowania minimum dwóch procesorów.Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci.Płyta główna powinna obsługiwać do 6TB pamięci RAM.Możliwość obsługi procesorów 128C
Chipset	<ul style="list-style-type: none">Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych.
Procesor	<ul style="list-style-type: none">Zainstalowane dwa procesory min. 16-rdzeniowe, min. 3.0GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 354 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocessorowej.
RAM	<ul style="list-style-type: none">Min. 512GB DDR5 RDIMM 5600MT/s,
Gniazda PCIe	<ul style="list-style-type: none">Min. trzy sloty PCIe



Cyberbezpieczny Samorząd

Zabezpieczenia pamięci RAM	<ul style="list-style-type: none">• Memory demand and patrol scrubbing,• Failed DIMM isolation,• Memory address parity protection
Kontroler RAID	<ul style="list-style-type: none">• Sprzętowy kontroler dyskowy, posiadający<ul style="list-style-type: none">◦ Min. 8GB nieulotnej pamięci cache,◦ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.◦ Wsparcie dla dysków samoszyfrujących
Dyski twarde	<ul style="list-style-type: none">• Zainstalowane:<ul style="list-style-type: none">◦ 2x dysk SSD SATA o pojemności min. 480GB, 2,5" Hot-Plug.• Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none">• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)• Czteroportowa karta sieciowa 1Gb Ethernet BaseT
Wbudowane porty	<ul style="list-style-type: none">• 4 porty USB w tym min:<ul style="list-style-type: none">◦ 1 port USB 3.0 z tyłu obudowy,◦ 1 port micro USB z przodu obudowy• 2 port VGA z czego jeden z przodu obudowy• Możliwość rozbudowy o port RS232
Video	<ul style="list-style-type: none">• Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200
Wentylatory	<ul style="list-style-type: none">• Redundantne
Zasilacze	<ul style="list-style-type: none">• Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium.
Elementy montażowe	<ul style="list-style-type: none">• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych



Cyberbezpieczny Samorząd

System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none">• 2 szt. Windows Server 2022 Standard licencja uprawniającą do korzystania z wszystkich rdzeni procesora• 10x licencja Windows Server 2022 RDS, User
Bezpieczeństwo	<ul style="list-style-type: none">• Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.• Moduł TPM 2.0• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem• Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	<ul style="list-style-type: none">• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:<ul style="list-style-type: none">○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;○ możliwość podmontowania zdalnych wirtualnych napędów;○ wirtualną konsolę z dostępem do myszy, klawiatury;○ wsparcie dla IPv6;○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;o integracja z Active Directory;o możliwość obsługi przez dwóch administratorów jednocześnie;o wsparcie dla dynamic DNS;o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwerao możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none">o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnejo Przesyłanie danych telemetrycznych w czasie rzeczywistymo Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerzeo Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none">• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych• integracja z Active Directory• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram• Szczegółowy opis wykrytych systemów oraz ich komponentów• Możliwość eksportu raportu do CSV, HTML, XLS, PDF• Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.• Grupowanie urządzeń w oparciu o kryteria użytkownika• Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach• Szybki podgląd stanu środowiska• Podsumowanie stanu dla każdego urządzenia• Szczegółowy status urządzenia/elementu/komponentu• Generowanie alertów przy zmianie stanu urządzenia.• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń• Integracja z service desk producenta dostarczonej platformy sprzętowej• Możliwość przejęcia zdalnego pulpitu• Możliwość podmontowania wirtualnego napędu• Kreator umożliwiający dostosowanie akcji dla wybranych alertów• Możliwość importu plików MIB• Przesyłanie alertów „as-is” do innych konsol firm trzecich• Możliwość definiowania ról administratorów• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów• Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
--	--



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

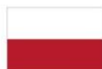


Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">• Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.• Zdalne uruchamianie diagnostyki serwera.• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.<ul style="list-style-type: none">○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none">• Monitoring:<ul style="list-style-type: none">○ ilość podłączonych oraz rozłączonych systemów○ stan podłączonych urządzeń○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia○ informacje o statusie gwarancji dla poszczególnych urządzeń○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.○ Monitoring parametrów serwerów z informacją o minimum:<ul style="list-style-type: none">▪ Obciążeniu procesora▪ Zużyciu pamięci RAM▪ Temperaturze procesorów▪ Temperaturze powietrza wlotowego▪ Zużyciu prądu▪ Zmianach w fizycznej konfiguracji serwera▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.○ Monitoring parametrów pamięci masowych z informacją o minimum:<ul style="list-style-type: none">▪ Opóźnieniach▪ IOPS▪ Przepustowości▪ Utylizacji kontrolerów▪ Pojemność całkowita i dostępna▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata▪ Informacje o poziomie redukcji danych
--	--



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Informacje o statusie replikacji oraz snapshotów○ Monitoring parametrów przełączników sieciowych z informacją o minimum:<ul style="list-style-type: none">▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny▪ Stanie komponentów: zasilacze, wentylatory▪ Podłączonych hostach▪ Ilości i statusu portów▪ Utylizacji procesora▪ Utylizacji poszczególnych portów▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.• Aktualizacja firmware<ul style="list-style-type: none">○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania• Raporty<ul style="list-style-type: none">○ Możliwość generowania raportów dla serwerów zawierających informację o:<ul style="list-style-type: none">▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej▪ Średnim obciążeniu: procesorów, pamięci RAM, IO,
--	---



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informacje o:<ul style="list-style-type: none">▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji○ Generowanie raportów do plików CSV i PDF• Cyberbezpieczeństwo<ul style="list-style-type: none">○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.• Wspierane urządzenia<ul style="list-style-type: none">○ Urządzenie Producenta dostarczane w ramach postępowania○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)• Wirtualny asystent<ul style="list-style-type: none">○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;• Możliwość rozszerzenia funkcjonalności<ul style="list-style-type: none">○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
--	--



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">• Inne<ul style="list-style-type: none">○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android• Certyfikaty<ul style="list-style-type: none">○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:<ul style="list-style-type: none">▪ ISO 27001▪ NIST Security and Privacy Controls for Federal Information Systems and Organization▪ CSA Cloud Control Matrix
Certyfikaty	<ul style="list-style-type: none">• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001• Serwer musi posiadać deklaracja CE.• Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	<ul style="list-style-type: none">• 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.
Wsparcie techniczne i oprogramowanie – w	Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

<p>formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</p>	<p>Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.</p> <p>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.</p> <p>Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.</p> <p>Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury.</p> <p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :</p> <ul style="list-style-type: none">• Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.• Predykcja analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.• Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.• upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,• możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :<ul style="list-style-type: none">a. o poprawkach i usprawnieniach dotyczących aktualizacjib. dacie wydania ostatniej aktualizacjic. priorytecie aktualizacjid. zgodność z systemami operacyjnymie. jakiego komponentu sprzętu dotyczy aktualizacjaf. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.
--	--



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.• - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)• dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml• raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Warunki gwarancji	<ul style="list-style-type: none">• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.• Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.• Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.• Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:<ul style="list-style-type: none">○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
--	---



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

3. Macierz wraz z oprogramowaniem do kopii bezpieczeństwa

Element konfiguracji	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5"
Przestrzeń dyskowa	Zainstalowane: 8x dyski SAS o pojemności min. 2.4TB, Hot-Plug 8x dyski SSD SAS o pojemności min. 1.92TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)
Kable/wkładki	4x kabel DAC 25GbE SFP28/SFP28 min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<p>Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Thin Provisioning	<p>Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.</p> <p>Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Tiering	<p>Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.</p> <p>Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.</p> <p>Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.</p>
Wewnętrzne kopie migawkowe	<p>Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p> <p>Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Wewnętrzne kopie pełne	<p>Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Migracja danych w obrębie macierzy	<p>Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać</p>



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Oprogramowanie do monitorowania – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: <ul style="list-style-type: none">• Monitoring:<ul style="list-style-type: none">○ ilość podłączonych oraz rozłączonych systemów○ stan podłączonych urządzeń○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia○ informacje o statusie gwarancji dla poszczególnych urządzeń○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
- Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
- Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
- Monitoring parametrów serwerów z informacją o minimum:
 - Obciążeniu procesora
 - Zużyciu pamięci RAM
 - Temperaturze procesorów
 - Temperaturze powietrza wlotowego
 - Zużyciu prądu
 - Zmianach w fizycznej konfiguracji serwera
 - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
 - Opóźnieniach
 - IOPS
 - Przepustowości
 - Utylizacji kontrolerów
 - Pojemność całkowita i dostępna
 - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata▪ Informacje o poziomie redukcji danych▪ Informacje o statusie replikacji oraz snapshotów○ Monitoring parametrów przełączników sieciowych z informacją o minimum:<ul style="list-style-type: none">▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny▪ Stanie komponentów: zasilacze, wentylatory▪ Podłączonych hostach▪ Ilości i statusu portów▪ Utylizacji procesora▪ Utylizacji poszczególnych portów▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.• Aktualizacja firmware<ul style="list-style-type: none">○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania• Raporty
--	--



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">○ Możliwość generowania raportów dla serwerów zawierających informację o:<ul style="list-style-type: none">▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej▪ Średnim obciążeniu: procesorów, pamięci RAM, IO,○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:<ul style="list-style-type: none">▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji○ Generowanie raportów do plików CSV i PDF● Cyberbezpieczeństwo<ul style="list-style-type: none">○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.● Wspierane urządzenia<ul style="list-style-type: none">○ Urządzenie Producenta dostarczane w ramach postępowania○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)● Wirtualny asystent
--	--



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;• Możliwość rozszerzenia funkcjonalności<ul style="list-style-type: none">○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.• Inne<ul style="list-style-type: none">○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android• Certyfikaty<ul style="list-style-type: none">○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:<ul style="list-style-type: none">▪ ISO 27001▪ NIST Security and Privacy Controls for Federal Information Systems and Organization▪ CSA Cloud Control Matrix
Wsparcie techniczne i oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.</p> <p>Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.</p> <p>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.</p> <p>Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.</p> <p>Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury.</p> <p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :</p> <ul style="list-style-type: none">• Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<ul style="list-style-type: none">• Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.• Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.• upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,• możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :<ul style="list-style-type: none">a. o poprawkach i usprawnieniach dotyczących aktualizacjib. dacie wydania ostatniej aktualizacjic. priorytecie aktualizacjid. zgodność z systemami operacyjnymie. jakiego komponentu sprzętu dotyczy aktualizacjaf. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.• - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)• dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml <p>raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem</p>
--	--



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

	<p>*.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.</p>
Warunki gwarancji	<p>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</p> <p>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia.</p> <p>Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p>



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii.

Charakterystyka usługi diagnostyki:

- Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
- Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
- Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
- Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
- Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

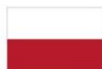
Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

Wykonawca zobowiązuje się do przeprowadzenia stacjonarnego wdrożenia dostarczonej macierzy w lokalizacji Zamawiającego. Zakres prac wdrożeniowych obejmuje w szczególności:

1. Przygotowanie szczegółowego planu wdrożenia - uzgodnienie z Zamawiającym sposobu instalacji, konfiguracji oraz terminu realizacji;
2. Montaż i konfigurację urządzeń - w tym podłączenie do infrastruktury sieciowej i dostosowanie ustawień do wymogów systemowych Zamawiającego;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

3. Integrację z istniejącym środowiskiem IT - przeprowadzenie testów kompatybilności, stabilności oraz bezpieczeństwa;
4. Przeszkolenie personelu - przekazanie wiedzy z zakresu bieżącej obsługi, podstawowej administracji oraz procedur konserwacyjnych, w tym także sposobu reagowania na ewentualne awarie;

Wszystkie działania zostaną przeprowadzone w uzgodnieniu z Zamawiającym, tak aby zapewnić poprawne i efektywne wdrożenie nowych urządzeń oraz bezpieczeństwo ich dalszego użytkowania.

b) Oprogramowanie

Rozwiązanie : XOPERO One Endpoint Agent - 100 stanowisk, XOPERO ONE Virtual Agent Virtual Machine x2, XOPERO ONE Virtual Agent per Socket x6, XOPERO ONE Cloud 2 TB lub równoważne spełniające parametry równoważności :

Zarządzanie i magazyny

1. Produkt dostępny w polskiej wersji językowej.
2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
9. System zarządzania nie może być oparty o relacyjne bazy danych.
10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn - serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykl..
15. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
16. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
17. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
18. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
19. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
20. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
21. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
22. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
23. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
24. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
25. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
26. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

27. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
28. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
29. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
30. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
31. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
32. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
33. Proces deduplikacji nie może posiadać pojedynczego punktu awarii
34. Proces deduplikacji realizowany jest blokiem o stałej wielkości.
35. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
36. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
37. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
38. System musi pozwalać na automatyczne aktualizacje oprogramowania.
39. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
40. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.
41. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
42. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
43. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

44. System musi pozwalać na gradację uprawnień administratorów - umożliwiał tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
45. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
46. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
47. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
48. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
49. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
50. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: G-F-S, Forever incremental,
51. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
52. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
53. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny
54. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
55. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
56. Możliwość generowania raportów dobowych w oparciu o harmonogram
57. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie UE)
58. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

59. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
60. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
9. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
10. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
11. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
12. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
13. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).



Cyberbezpieczny Samorząd

Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej 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 środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket.
5. System musi umożliwiać zabezpieczanie środowisk Jira



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Anty-ransomware i bezpieczeństwo

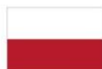
1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.

Licencjonowanie i wsparcie techniczne

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
3. Możliwość zgłaszania ticketów supportowych przez formularz zgłoszeniowy znajdujący się na oficjalnej stronie www producenta.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
7. Dostęp do wsparcia technicznego producenta powinno obowiązywać co najmniej do 30 czerwca 2026 roku.
8. Sposób licencjonowania opiera się na:
 - Ilości serwerów/endpointów- dla fizycznych urządzeń,
 - Ilości fizycznych hostów - dla środowisk wirtualnych,
 - Ilości repozytoriów - dla GIT.
 - Ilość userów - dla Jira.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- ilość maszyn wirtualnych (opcja dodatkowa)
- 9. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej:
 - 100 stacji roboczych,
 - Nielimitowanej ilości maszyn wirtualnych w obrębie fizycznych serwerów stanowiących podstawy do wirtualizacji (łącznie 6 socketów)
 - 2 maszyny wirtualne
- 10. Licencje powinny umożliwiać korzystanie z przestrzeni chmurowej dostarczonej bezpośrednio przed producenta, min. 2TB przez cały okres trwania wsparcia technicznego dostarczonej na oprogramowanie.

Wdrożenie:

- o Wdrożenie może się odbyć w formie zdalnej,
- o Wdrożenie musi zostać przeprowadzone bezpośrednio przez producenta oprogramowania lub certyfikowanego przez producenta inżyniera,
- o Wdrożenie musi się odbyć w języku polskim,
- o Wdrożenie musi obejmować podstawowe szkolenie z obsługi oprogramowania.
- o Czas wdrożenia - 8 godzin
- o Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania

Szkolenie:

- o Szkolenie realizowane jest bezpośrednio przez producenta oprogramowania lub certyfikowanego przez producenta trenera,
- o Szkolenie może zostać zrealizowane w formie zdalnej,
- o Komunikacja podczas szkolenia musi odbywać się w języku polskim,
- o Czas szkolenia - 8 godzin

4. Serwer NAS



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Procesor	Jeden 8-rdzeniowy/16-wątkowy procesor AMD Ryzen™ 7 lub równoważny procesor ośmiordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 25000 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/high_end_cpus.html
Obudowa	Rack 2U o wymiarach nie większych niż, 89× 483 × 565 mm (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK
Pamięć RAM	32 GB UDIMM DDR5 z opcją rozszerzenia do 192GB RAM
Ilość obsługiwanych dysków	12 dysków 3,5-calowych 3,5/2,5 dyski SATA
Ilość zainstalowanych dysków	10 dysków HDD o min. pojemności 12TB, cache 512MB wspierających funkcjonalność NASware 2 dyski SSD M.2 NVMe o min. pojemności 1TB. Dyski klasy NAS do pracy 24/7
Interfejsy sieciowe	2 porty 1Gigabit sieci Ethernet (RJ45) 2 porty 10GbE (10GBase-T)
Porty	2 gniazda typu A USB 3.2 Gen 2 10 Gb/s
Porty PCIe	3 gniazda PCIe Gen4 Jeden z portów obsadzony kartą posiadającą 2 gniazda PCIe 2280 M.2 SSD oraz 2 porty 10GbE RJ45 – na gniazdach M.2 zainstalowane dyski M.2 NVMe o min. pojemności 500GB. Dyski klasy NAS do pracy 24/7
Wskaźniki LED	Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej
Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity



Cyberbezpieczny Samorząd

Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.
Stacja monitoringu	Tak, w standardzie 8 darmowych licencji na podłączenie kamer.
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP
Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog Container Station
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	24 miesiące gwarancji producenta na NAS
Waga	Nie więcej niż 14 kg (netto)



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

System plików	Dyski wewnętrzne ZFS, EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń (CIFS)	5000
Max liczba migawek	65536
Zasilanie	Redundantne 550 W (x2), 200–240 V

5. Zarządzalne urządzenie sieciowe - 1 szt.

Przedmiotem zamówienia jest dostawa fabrycznie nowego, nieużywanego urządzenia typu Next-Generation Firewall (NGFW) wraz z niezbędnymi akcesoriami i licencjami.

Minimalne wymagania techniczne

Parametr	Minimalne wymagania
Typ urządzenia	Next-Generation Firewall (NGFW) z funkcjami IPS, AVC (Application Visibility and Control), filtrowaniem URL, ochroną przed złośliwym oprogramowaniem (AMP) lub równoważne.



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską





Cyberbezpieczny Samorząd

Architektura	Procesor klasy x86 (np. Intel) z wydajnością odpowiednią do obsługi jednoczesnej pracy wszystkich funkcji bezpieczeństwa. RAM: min. 32 GB, Dysk: min. 200 GB SSD.
Wydajność	<ul style="list-style-type: none">- Przepustowość z włączonym IPS i AVC: min. 3 Gb/s- Przepustowość VPN (IPSec): min. 1,4 Gb/s- Min. 28 000 nowych połączeń/s (AVC)- Min. 600 000 jednoczesnych połączeń (AVC).
Interfejsy sieciowe	<ul style="list-style-type: none">- Min. 8 × 10/100/1000Base-T (RJ-45)- Min. 2 × SFP/SFP+ (kompatybilne w dół do 1Gb)- Min. 2 × 10Gb SFP+- 1 × RJ-45 (port zarządzający).
Funkcje bezpieczeństwa	<ul style="list-style-type: none">- Zaawansowane IPS/IDS- Kontrola aplikacji (Application Control)- Filtrowanie URL- SSL/TLS Inspection- Ochrona przed złośliwym oprogramowaniem i automatyczne aktualizacje sygnatur.
Zarządzanie	<ul style="list-style-type: none">- Interfejs webowy (HTTPS) + CLI (SSH)- Możliwość logowania (syslog, SNMP)- Centralne zarządzanie (np. Cisco FMC) lub równoważne.
Wymiary i montaż	<ul style="list-style-type: none">- 1U, rack 19", przepływ powietrza: przód-tył- Wymiary ~44 cm × 27 cm × 4,5 cm- Masa ~4 kg
Zasilanie	<ul style="list-style-type: none">- AC 100–240 V, 50/60 Hz, moc do 100 W lub równoważne- Zasilacz wewnętrzny.
Zgodność z normami	- CE, EN 60950-1 / EN 55032 / EN 61000-3-2 / EN 61000-3-3
Licencje i subskrypcje	<i>Patrz. Poniżej tabeli „szczegółowe wymagania licencyjne”</i> - Aktualizacje baz sygnatur i poprawki bezpieczeństwa przez cały okres ważności.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Szczegółowe wymagania licencyjne

1. Licencja na urządzenie:

" Zapewnienie subskrypcji obejmującej m.in. Threat (IPS), URL Filtering, Advanced Malware Protection (AMP) przez okres obowiązywania do 30.06.2026 r.

" Umożliwienie bieżącej aktualizacji baz sygnatur, reguł bezpieczeństwa i modułów ochrony.

2. Licencja serwisowa:

" Świadczenie serwisu i wsparcia w zakresie sprzętu i oprogramowania NGFW przez okres obowiązywania do 30.06.2026 r.

" Dostęp do poprawek, aktualizacji oprogramowania (OS, firmware), a także wsparcie techniczne producenta w formie zgłoszeń telefonicznych i e-mailowych.

Gwarancja i wsparcie serwisowe

1. Urządzenie i licencje mają być objęte gwarancją i wsparciem co najmniej do 30.06.2026 r.

2. Wsparcie serwisowe w ramach zawartych umów powinno obejmować:

" możliwość zgłaszania usterek telefonicznie i elektronicznie,

" czas reakcji na zgłoszenia (SLA) nie dłuższy niż do końca następnego dnia roboczego (NBD) - o ile Zamawiający nie określi inaczej w SWZ,

" dostęp do aktualizacji oprogramowania i baz sygnatur bezpieczeństwa.

Wdrożenie i szkolenie

Wykonawca zobowiązuje się do przeprowadzenia stacjonarnego wdrożenia urządzenia w lokalizacji Zamawiającego. Zakres prac wdrożeniowych obejmuje w szczególności:

1. Przygotowanie szczegółowego planu wdrożenia - uzgodnienie z Zamawiającym sposobu instalacji, konfiguracji oraz terminu realizacji;

2. Montaż i konfigurację urządzenia - w tym podłączenie do infrastruktury sieciowej i dostosowanie ustawień do wymogów systemowych Zamawiającego;

3. Integrację z istniejącym środowiskiem IT - przeprowadzenie testów kompatybilności, stabilności oraz bezpieczeństwa;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

4. Przeszkolenie personelu - przekazanie wiedzy z zakresu bieżącej obsługi, podstawowej administracji oraz procedur konserwacyjnych, w tym także sposobu reagowania na ewentualne awarie;
5. Dokumentację powdrożeniową - obejmującą opis konfiguracji, instrukcje eksploatacyjne oraz zalecenia dotyczące utrzymania i bezpieczeństwa.

Wszystkie działania zostaną przeprowadzone w uzgodnieniu z Zamawiającym, tak aby zapewnić poprawne i efektywne wdrożenie nowych urządzeń oraz bezpieczeństwo ich dalszego użytkowania.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA