

Załącznik nr 4 do SWZ**OPIS PRZEDMIOTU ZAMÓWIENIA****ZAMÓWIENIE JEST PODZIELONE NA 2 CZĘŚCI:****Część I Zamówienia: Modernizacja Data Center, system kopii zapasowej:****1. Przedmiotem zamówienia jest:**

1. Dostawa 2 fabrycznie nowych serwerów, nie finansowanych wcześniej z krajowych lub unijnych funduszy projektowych;
2. Dostawa macierzy dyskowej, nie finansowanych wcześniej z krajowych lub unijnych funduszy projektowych;
3. Dostawa podzespołów serwerowych do aktualnie posiadanych serwerów przez zamawiającego, nie finansowanych wcześniej z krajowych lub unijnych funduszy projektowych;
4. Dostawa wymaganego oprogramowania – dwie dodatkowe i niezależne licencje Windows Server 2025 Standard - 16 Core License Pack;
5. Konfiguracja, instalacja nowych podzespołów w serwerach zamawiającego - Lenovo SR630 V2 (ThinkSystem), SN: J7011YP8, J7012ZFK;
6. Konfiguracja, instalacja macierzy dyskowej;
7. Wdrożenie oraz konfiguracja środowiska wirtualizacji w środowisku IT Zamawiającego;
8. Wsparcie w migracji obecnie posiadanych systemów
9. Dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego systemu
10. dostawa serwera fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych,
11. dostawa macierzy NAS fabrycznie nowej, nie finansowanej wcześniej z krajowych lub unijnych funduszy projektowych,
12. dostawa streamera LTO fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych,
13. konfiguracja, instalacja serwera,
14. konfiguracja, instalacja macierzy NAS,
15. konfiguracja, instalacja streamera LTO,
16. dostawa sytemu kopii zapasowych – licencja wieczysta z rocznym wsparciem producenta umożliwiające kopie 25 VM, 5 maszyn fizycznych oraz 50 PC,
17. wdrożenie oraz konfiguracja systemu kopii zapasowych w środowisku IT Zamawiającego,
18. dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego rozwiązania.

2. Termin realizacji zamówienia:

Dostawa sprzętu w ramach Części I Zamówienia w terminie do 42 dni od dnia zawarcia umowy.

3. Wymagania wobec Wykonawcy:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie warunki określone w załączniku nr 6 do SWZ:

- w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizował co najmniej dwie dostawy o podobnym charakterze (przez co Zamawiający rozumie dostawy sprzętu serwerowego oraz sieciowego wraz z wdrożeniem oprogramowania infrastruktury sprzętowej systemów informatycznych na kwotę minimum 250 000,00 zł brutto każde zadanie) wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

tych dokumentów – oświadczenie Wykonawcy Przez jedno zamówienie (dostawę) rozumie się dostawę będącą przedmiotem jednostkowej, odrębnej umowy

4. Wymagania szczegółowe Zamawiającego:

Zestawienie wymaganych parametrów technicznych – macierz dyskowa typ 1 (1 sztuk/a)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19” rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalację 24 dysków 2.5”. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active (dual-active) posiadające łącznie minimum osiem portów iSCSI BaseT 10Gb/s.
Procesory	Intel Xeon Processor
Cache	16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami. Całkowita ilość cache 32GB.
Dyski	Zainstalowane 5 dysków Hot-Plug o pojemności nie mniejszej niż 1.92TB SSD SAS 12Gb 1DWPD. Zainstalowane 6 dysków Hot-Plug o pojemności nie mniejszej niż 2,4 TB SAS ISE 12Gb/s 10 tys. obr./min. Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych tak by uzyskać łącznie nie mniej niż 264 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie/ Funkcjonalność	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Wentylatory	Redundantne

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

Zasilacze	Redundantne, Hot-Plug maksymalnie 580W każdy.
Diagnostyka	Poprzez kartę zarządzającą
Certyfikaty	Macierz musi być wyprodukowany zgodnie z normą ISO-9001:2015 Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta – dokumenty potwierdzające załączyć do oferty Serwer musi posiadać deklaracja CE.
Warunki gwarancji	Cztery lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji do 7 lat. W przypadku awarii dyski zostają u zamawiającego.
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.

Zestawienie wymaganych parametrów technicznych dla podzespołów serwerowych – Lenovo SR630 V2 (ThinkSystem), SN: J7011YP8, J7012ZFK;

Parametr	Ilość
16GB TruDDR4 3200 MHz (2Rx8 1.2V) RDIMM	16
Performance Fan Option Kit	2
ST650 V2 Intel Xeon Silver 4309Y 8C 105W 2.8GHz Processor Option Kit w/o Fan	2

Oferowany podzespół musi być zgodny z listą kompatybilności producenta (Lenovo) urządzenia dostarczoną przez producenta.

Zaproponowany przez wykonawcę procesor musi być dokładnie ten sam który jest zainstalowany w serwerze by zapewnić kompatybilność i stabilność środowiska.

5. Zestawienie wymaganych parametrów technicznych odnośnie systemów operacyjnych:

- 1) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
- 2) Wbudowane wsparcie instalacji i pracy na wolumenach które:
 - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
 - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- 3) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 4) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- 5) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
- 6) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- 7) Wbudowana zaporą internetowa (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 8) Graficzny interfejs użytkownika.
- 9) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- 10) Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
- 11) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 12) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 13) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
- 14) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - c) podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - d) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - e) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- 15) Zdalna dystrybucja oprogramowania na stacje robocze.
- 16) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
- 17) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - a) dystrybucję certyfikatów poprzez http,
 - b) konsolidację CA dla wielu lasów domeny,
 - c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
- 18) Szyfrowanie plików i folderów.
- 19) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- 20) Serwis udostępniania stron WWW
- 21) Wsparcie dla protokołu IP w wersji 6 (Ipv6).
- 22) Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

6. Wymagane prace wdrożeniowe

1. Dostarczenie sprzętu wraz z konfiguracją:

- a) Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego
- b) Zamawiający zobowiązuje się do wskazania osób kontaktowych, świadczących wsparcie dla aplikacji dziedzinowych, celem ich migracji do nowego środowiska serwerowego.
- c) Dedykowane wsparcie aplikacji dziedzinowych realizuje migrację aplikacji do nowego środowiska na wniosek Zamawiającego
- d) Podłączenie macierzy do infrastruktury elektrycznej i sieciowej Zamawiającego
- e) Konfiguracja serwera, polegająca na, dołożeniu podzespołów, nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- f) Konfiguracja macierzy, polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowemu do najnowszej zalecanej przez producenta wersji
- g) Konfiguracja środowiska wirtualizacji
- h) Migracja VM do nowo zakupionej macierzy
- i) Przekazanie dostępów Zamawiającemu
- j) Testy po uruchomieniu środowiska wirtualnego polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego
- k) Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów
- l) Serwery typu 1 i 2 nie wymagają prac wdrożeniowych.

Zestawienie wymaganych parametrów technicznych – serwer (1 sztuka)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5" Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	<ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	<ul style="list-style-type: none"> Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 95.1 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocessorowej.
Pamięć RAM	<ul style="list-style-type: none"> 2x16GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s.
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"> 4x dyski HDD SATA o pojemności min. 12TB, Hot-Plug. Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCIe	<ul style="list-style-type: none"> Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Zainstalowane min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT Zainstalowana kompatybilna karta rozszerzeń HBA SAS (4 Ports Quad), 12 Gb/s
Wbudowane porty	<ul style="list-style-type: none"> min. 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 1 port VGA na tylnym panelu, 1 port RS232

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

Karta graficzna	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> Windows Server 2025 Standard - 16 Core License Pack
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 w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 V3 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; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla automatycznej rejestracji DNS wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<ul style="list-style-type: none"> o 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 zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o 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,

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<p>występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</p> <ul style="list-style-type: none"> o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o 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. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o 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

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<ul style="list-style-type: none"> ♣ 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 ♣ 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,
--	---

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<ul style="list-style-type: none"> o 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 o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> o 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. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiającą wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia <ul style="list-style-type: none"> o Urządzenie Producenta dostarczane w ramach postępowania o 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"> o 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"> o 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"> o Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
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.

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<p>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.</p> <ul style="list-style-type: none"> 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.
Warunki gwarancji	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 4 lat. Wymagana możliwość zachowania dysku twardego w ramach świadczonej usługi wsparcia serwisowego dla sprzętu, obejmująca 4-letni okres wsparcia serwisowego z gwarancją producenta. Usługa ma na celu umożliwienie zamawiającemu zachowania nośników danych (dysków twardych) po ich awarii. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 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 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 wparciem 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 zgłoszenia 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

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<p>harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.</p> <ul style="list-style-type: none"> o 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. <p>Wykonawca zobowiązuje się zapewnić 10 godzin (rocznie) wsparcia technologiczno-konsultacyjnego dla oferowanego sprzętu w okresie 2 lat. Usługa obejmuje doradztwo i rozwiązywanie problemów technicznych urządzenia, dostarczonego oprogramowania oraz powiązanych z nim komponentów sieci. Szczegółowe warunki wsparcia zostaną określone w załączniku opisującym zakres i sposób świadczenia usługi</p>
--	--

Zestawienie wymaganych parametrów technicznych – macierz NAS (1 sztuka)

Typ urządzenia	Serwer NAS
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark w lipcu 2022 co najmniej 4580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA
Porty zewnętrzne	Minimum: <ul style="list-style-type: none"> • 2 porty USB 3.2.1 • 1 eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: <ul style="list-style-type: none"> • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8
Wentylator obudowy	Min. 2 wentylatory 80 mm x 80 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: <ul style="list-style-type: none"> • Wewnętrzny: Btrfs, ext4

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

	<ul style="list-style-type: none"> Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	<ul style="list-style-type: none"> Maksymalny rozmiar pojedynczego wolumenu: 108 TB Minimalny liczba wewnętrznych wolumenów: 64 Minimalny liczba obiektów iSCSI Target: 128 Minimalny liczba jednostek iSCSI LUN: 256 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	<ul style="list-style-type: none"> Minimalna liczba kont użytkowników: 2 048 Minimalna liczba grup użytkowników: 256 Minimalna liczba folderów współdzielonych: 512 Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Oprogramowanie	<ul style="list-style-type: none"> Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.
Konserwacja	<ul style="list-style-type: none"> Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack
Zasilanie	<ul style="list-style-type: none"> Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

Gwarancja	<p>Wykonawca udzieli gwarancji:</p> <ul style="list-style-type: none"> • 3 lata na urządzenie główne • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack
-----------	--

Zestawienie wymaganych parametrów technicznych – Dysk Typ1 - (8 sztuk)

Parametr	Wartość
Pojemność	6 TB
Format	3.5"
Interfejs	SATA 6 Gb/s
Prędkość obrotowa	5,400 obr./min
Maks. prędkość przesyłu danych	202 MB/s
Gwarancja	3 lat
Zużycie energii w trybie aktywnego bezczynności (typowe)	3,4 W
Zakres temperatury podczas pracy	0°C do 65°C (32°F do 149°F)
Zakres temperatury podczas spoczynku	-40°C do 70°C (-40°F do 158°F)

Zestawienie wymaganych parametrów technicznych – biblioteka LTO (1 sztuka)

Lp.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Wykorzystana technologia	LTO Ultrium wspierająca technologię partycjonowania nośników.
2.	Obudowa	Typu rack 19". Wysokość maksymalnie 1U - wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem. Urządzenie musi mieć możliwość instalowania w tej samej obudowie różnych generacji napędów LTO (minimum od LTO-6 wzwyż).
3.	Wbudowany napęd	LTO-8 wyposażony w dwa złącza mSAS SFF-8088. Urządzenie musi mieć możliwość instalowania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasety oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2
4.	Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy podzielone na dwa magazynki (urządzenie musi być dostarczone z kompletem magazynków). Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot musi odbywać się bez konieczności wysuwania całego magazynka.
5.	Pojemność	Pojemność bez kompresji – minimum 96TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-8
6.	Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

		IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówno poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
7.	Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI
8.	Obsługa urządzenia	Wymagana możliwość wymiany napędu, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki. Wsparcie funkcjonalności Air Gap (izolacji powietrznej)
9.	Wypożyczenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli: 1x zasilając, 1x komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. W przypadku, gdyby serwer nie dysponował odpowiednim kontrolerem, należy taki dostarczyć wraz z urządzeniem – interfejs kontrolera: dual SAS 12Gb). Wraz z urządzeniem należy dostarczyć także zestaw 15-tu identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 12TB oraz jeden nośnik czyszczący wyposażonych w unikalne naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty.
10.	Kompatybilność	Urządzenie musi być w pełni kompatybilne z aplikacją Veeam Backup and Replication, która będzie wykorzystywana do backupu danych – kompatybilność musi być potwierdzona odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty
11.	Gwarancja	<p>36 miesięcy z szybkiej wymiany całego urządzenia lub komponentów w czasie do 48 godz. (dni robocze) od momentu zgłoszenia uszkodzenia. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9 z czasem reakcji do 12 godzin od zgłoszenia. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Do oferty należy dołączyć pisemne oświadczenia wystawione przez producenta o gwarancji świadczonej w rygorze 5x9xNBD realizowanej przez producenta wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy.</p> <p>Wykonawca zobowiązuje się zapewnić 10 godzin (rocznie) wsparcia technologiczno-konsultacyjnego dla oferowanego sprzętu w okresie 2 lat. Usługa obejmuje doradztwo i rozwiązywanie problemów technicznych urządzenia, dostarczonego oprogramowania oraz powiązanych z nim komponentów sieci. Szczegółowe warunki wsparcia zostaną określone w załączniku opisującym zakres i sposób świadczenia usługi</p>

Zestawienie wymaganych parametrów technicznych – system do Backupu

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

1. Wymagania ogólne

- a. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions> i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
- b. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- c. Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.
- d. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

2. Całkowite koszty posiadania

- a. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- b. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- c. 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
- d. 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.
- e. 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 to takiej puli.
- f. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
- g. Oprogramowanie musi wspierać niezmiennność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
- h. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- i. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
- j. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- k. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
- l. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- m. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji
- n. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- o. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
- p. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
- q. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
- r. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
- s. Oprogramowanie musi posiadać integracje z systemami typu SIEM
- t. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

3. Wymagania RPO

- a. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- b. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- c. 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 z dokładnością do pojedynczego datastora
- d. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
- e. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- f. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
- g. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- h. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
- i. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- j. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
- k. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- l. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.
- m. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- n. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
- o. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

4. Wymagania RTO

- a. 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 środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- b. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- c. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych 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
- d. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
- e. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
- f. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- g. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
- h. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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
- i. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- j. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
- k. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
- l. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- m. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
- n. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- o. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
- p. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
- q. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
- r. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
- s. Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
- t. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
- u. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
- v. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
- w. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
- x. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
- y. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

5. Ograniczenie ryzyka

- a. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- b. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
- c. 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
- d. 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.
- e. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
- f. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
- g. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- h. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
6. Zestawienie wymaganych parametrów technicznych odnośnie systemów operacyjnych:
- 1) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
 - 2) Wbudowane wsparcie instalacji i pracy na wolumenach które:
 - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
 - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 - 3) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - 4) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - 5) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
 - 6) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - 7) Wbudowana zaporę internetową (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 - 8) Graficzny interfejs użytkownika.
 - 9) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
 - 10) Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
 - 11) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 - 12) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
 - 13) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
 - 14) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - c) podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - d) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - e) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - 15) Zdalna dystrybucja oprogramowania na stacje robocze.
 - 16) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
 - 17) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - a) dystrybucję certyfikatów poprzez http,
 - b) konsolidację CA dla wielu lasów domeny,
 - c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- 18) Szyfrowanie plików i folderów.
- 19) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- 20) Serwis udostępniania stron WWW
- 21) Wsparcie dla protokołu IP w wersji 6 (Ipv6).
- 22) Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

5. Wymagane prace wdrożeniowe

1) Dostarczenie sprzętu wraz z konfiguracją

- a) Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego
- b) Podłączenie serwera, macierzy, biblioteki LTO do infrastruktury elektrycznej i sieciowej Zamawiającego
- c) Wstępna konfiguracja serwera, macierzy, biblioteki LTO polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
- d) Przekazanie dostępów Zamawiającemu
- e) Testy po uruchomieniu środowiska polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego
- f) Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów

2) Wdrożenie backup

- a) instalacja oprogramowania do kopii zapasowych na zasobie wskazanym przez Zamawiającego;
- b) skonfigurowanie repozytorium kopii zapasowych wskazanego przez Klienta
- c) zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do kopii zapasowych dla przynajmniej 6 maszyn wirtualnych i 40 stacji roboczych;
- d) Podłączenie do Gminnego Centrum Przetwarzania Danych jednostek podległych - BOOS, ŚDS oraz MGOPS. Konfiguracja i archiwizacja ich repozytoriów. Każda z jednostek zadeklarowała 1TB danych do archiwizacji na zasobach UG.
- e) przeprowadzenie testów akceptacyjnych poprawności działania operacji, kopii zapasowych i odzyskiwania danych;
- f) konfiguracja powiadomień systemu kopii zapasowej oraz weryfikacja ich działania.

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

Część II Zamówienia: Bezpieczeństwo na urządzeniach końcowych, SOC dla obszaru XDR:

1. Przedmiotem zamówienia jest:
 1. Wdrożenie centralnie zarządzanego rozwiązania antywirusowego w środowisku chmurowym oraz rozszerzenie o rozwiązanie klasy XDR posiadającego niezależną konsolę administracyjną – szczegóły wymaganych funkcji oraz możliwości zostały opisane w punkcie 1.3 niniejszego dokumentu.
 2. Instalacja wymaganych do prawidłowego działania agentów i/lub aplikacji na stacjach końcowych, które mają być objęte ochroną antywirusową wraz z funkcją XDR – stacje zostaną wskazane przez Zamawiającego.
 3. Testy poprawności wdrożonego rozwiązania potwierdzone pisemnie przez Zamawiającego oraz Wykonawcę.
 4. Świadczenie usługi SOC w oparciu o systemy klasy EDR/XDR posiadane w infrastrukturze IT Zamawiającego.
2. Termin realizacji Części II Zamówienia:
Zamówienie będzie realizowane przez okres 12 miesięcy od dnia zawarcia umowy.
3. Wymagania wobec Wykonawcy:
O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie warunki określone w załączniku nr 6 do SWZ.
4. Wymagane prace wdrożeniowe:
 1. Wdrożenie oraz dostosowanie konfiguracji usług zgodnie z najlepszymi praktykami, zapewniającymi prawidłową funkcjonalność rozwiązania.
 2. Implementacja licencji w rozwiązaniu – dodatkowo rozszerzenie rozwiązania antywirusowego o rozwiązanie klasy XDR, w formie niezależnej konsoli administracyjnej
 3. Instalacja dostarczonych licencji i przypisanie ich dla poszczególnych użytkowników
 4. Instalacja na stacjach roboczych/serwerach agentów i/lub aplikacji wymaganych do poprawnego działania oraz komunikacji oferowanego rozwiązania
 5. Prace wdrożeniowe muszą odbyć się po ustaleniu z Zamawiającym harmonogramu wdrożenia, który musi być przedstawiony Zamawiającemu do 4 tygodni od czasu podpisania umowy.
5. Szczegółowe wymagania odnośnie usługi:
 1. Usługa wsparcia ma być realizowana w następujących obszarach:
 - a) Monitorowanie i reakcja – monitorowanie i reakcja na zagrożenia mogące stanowić zagrożenie dla ciągłości działania infrastruktury IT. W ramach usługi musi być realizowane:
 - Monitorowanie musi być w trybie ciągłym - codzienne,
 - Zarządzanie wkluczeniami na bazie ustaleń z Zamawiającym,
 - Blokowanie zagrożeń - blokowanie potencjalnie niebezpiecznych zdarzeń i informowanie Zamawiającego o podjętych działaniach,
 - Minimalizacja ilości fałszywych alarmów generowanych przez zaakceptowane przez Zamawiającego zdarzenia.
 - b) Ocena i klasyfikacja incydentów bezpieczeństwa – analiza i informacja w zakresie rozwiązywania incydent bezpieczeństwa w infrastrukturze IT,
 - Każdorazowa analiza zdarzeń dla zagrożeń na poziomie Warning i Threat

„DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD”

- Ocena poziomu istotności zagrożeń w odniesieniu do infrastruktury i procesów Zamawiającego.
 - Klasyfikacja zagrożeń zgodnie z punktacją systemu EDR/XDR, wskazująca na konieczność podjęcia działań.
 - c) Raportowanie – cykliczne raportowanie informacji na temat zarządzanych incydentów bezpieczeństwa. Raporty powinny być dostarczane w następujących cyklach:
 - Raportowanie tygodniowe – raporty ilościowe z wykrytych zdarzeń,
 - Raportowanie miesięczne - podsumowanie i analiza wykrytych zdarzeń oraz zastosowanych polityk bezpieczeństwa
 - 2) Rozpoczęcie współpracy i wdrożenie usługi SOC musi wiązać się z zapoznaniem się na temat stanu infrastruktury IT zamawiającego oraz procesów biznesowych w ramach których pracują systemy i urządzenia objęte system klasy EDR/XDR Zamawiającego przez Oferenta, dopuszczając się realizację procesu inwentaryzacji zdalnie lub w siedzibie Zamawiającego wraz z osobą odpowiedzialną za obszar IT po stronie Zamawiającego
 - 3) Usługa ma być realizowana w godzinach 8:00 – 16:00 w dni robocze, dla zdarzeń krytycznych w trybie 24/7/365.
 - 4) Czas reakcji na incydenty do 1 godziny w dni robocze w godzinach 8:00 – 16:00.
 - 5) Kontakt w ramach usługi wsparcia musi być realizowany za pośrednictwem infolinii, komunikacji e-mail lub systemu formularzy, przy czym Zamawiający wymaga utrzymania minimum 2 form kontaktu z wcześniej wymienionych
6. Wymagania formalne do Zamówienia „Dostawa sprzętu w ramach projektu Cyberbezpieczny Samorząd”:
1. Specyfikacje i parametry techniczne wszystkich wymaganych przez Zamawiającego i opisanych w niniejszym Opisie Przedmiotu Zamówienia sprzętów i rozwiązań informatycznych,
 2. Oświadczenie o zgodności oferty z wymaganiami SWZ – oświadczenie sporządzone samodzielnie przez Wykonawcę,
 3. Potwierdzenie posiadania niezbędnych zasobów technicznych i kadrowych do realizacji usługi – oświadczenie sporządzone samodzielnie przez Wykonawcę,
 4. Wykazanie doświadczenia w świadczeniu dostaw i usług o podobnym charakterze – Załącznik nr 6 do SWZ