Cyberbezpieczny Samorząd

Załącznik nr 2 do postępowania,
znak sprawy: **OSO.1333.36.2024**

FORMULARZ OFERTY

dla zapytania o wartości poniżej kwoty 130 000,00 złotych netto w Urzędzie Gminy Marklowice, wprowadzonego Zarządzeniem Nr 0050.5.2021 Wójta Gminy Marklowice z dnia 04.01.2021 roku.

Dane dotyczące Wykonawcy

Nazwa .....

Siedziba .....

Nr telefonu/faks/e-mail .....

NIP .....

REGON .....

reprezentowany przez:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Dane dotyczące Zamawiającego

Gmina Marklowice

ul. Wyzwolenia 71, 44-321 Marklowice

Zobowiązania Wykonawcy

1. Zobowiązuję się wykonać przedmiot zamówienia pn:" Dostawa serwera kopii bezpieczeństwa wraz z oprogramowaniem wykonującym kopie bezpieczeństwa serwera fizycznego na którym pracują maszyny wirtualne oraz kopii z pięćdziesięciu stacji roboczych w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd" (Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa. Fundusze Europejskie na Rozwój Cyfrowy 2021-2027)."zgodnie z opisem przedmiotu zamówienia.

Łączna oferowana cena netto:	
Słownie netto:	
Łączna oferowana cena brutto:	
Słownie brutto:	

2. Oświadczamy, że zapoznaliśmy się ze Szczegółowym Opisem Przedmiotu Zamówienia oraz zdobyliśmy konieczne informacje do przygotowania oferty.

3. Oświadczamy, iż uważamy się za związanych niniejszą ofertą przed okres 30 dni licząc od daty wyznaczonej na składanie ofert.

4. Oświadczamy, że zapoznaliśmy się z postanowieniami zawartymi we wzorze umowy i zobowiązujemy się, w przypadku wyboru naszej oferty jako najkorzystniejszej, do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.

5. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust. 1 w związku z art. 7 ust.9 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

6. Poniżej proponujemy następujące urządzenie wraz z oprogramowaniem:

……..

……..

……..

Które spełniają następujące pozycje:

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne	Spełnia Tak / Nie
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.	
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 125W. Wymagana ilość rdzeni dla procesora – 8. Minimalna częstotliwość pracy procesora 2.6GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora dla proponowanego serwera nie powinien być nizszy niż 172 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Jednocześnie wynik wydajności procesora dla proponowanego serwera nie powinien być nizszy niż 13.9 punkty base w teście SPECspeed 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej.	
Liczba procesorów	2	
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania minimum dwóch procesorów wykonujących 64-bitowe instrukcje	
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w	

	kościach min 64Gb. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.	
Zabezpieczenie pamięci	ECC, SDDC, ADDDC, Memory Mirroring	
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera.	
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum dziesięć dysków SATA 3,5” o pojemności minimum 8TB każdy Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym raid . Nie dopuszcza się rozwiązania, w którym dyski M.2 zajmują którykolwiek ze slotów PCIe. Wymagany jest wewnętrzny slot na kartę Micro SD.	
Kontroler dyskowy	Zainstalowany sprzętowy kontroler SAS 12Gb do obsługi dysków min 12 dysków wewnętrznych. Kontroler musi obsługiwać poziomy RAID - 0/1/10.	
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium.	
Interfejsy sieciowe	Zainstalowana czteroportowa karta 10Gb Base-T. Karta nie może zajmować żadnego ze slotów PCIe.	
Dodatkowe sloty I/O	Serwer w momencie dostawy musi posiadać 3 sloty PCIe 4.0 z czego jeden x16. Serwer musi posiadać jeden slot OCP 3.0 na potrzeby instalcji karty sieciowej.	
Dodatkowe porty	• z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA. • z tyłu obudowy: 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera. Możliwość instalacji dodatkowego redundantnego portu RJ45 służacego do zarządzania, w slocie OCP zamiast karty sieciowej.	
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1	
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna	

- Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja
- Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
- Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.
- Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3
- Update systemowego firmware
- Monitoring i możliwość ograniczenia poboru prądu
- Zdalne włączanie/wyłączanie/restart
- Zapis video zdalnych sesji
- Podmontowanie lokalnych mediow z wykorzystaniem Java client
- Przekierowanie kosnoli szeregowej przez IPMI
- Zrzut ekranu w momencie zawieszenia systemu
- Możliwość przejęcia zdalnego ekranu
- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera
- Możliwość mapowania obrazów ISO z lokalnego dysku operatora
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
- Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.

- Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.

- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.

- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.

- Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.

Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:
- zarzadzanie infrastruktura serwerówi storage bez udziału dedykowanego agenta
- przedstawianie graficznej reprezentacji zarządzanych urządzeń

	- możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu	

	na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.	
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.	
Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz.	
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.	
Wspierane systemy operacyjne:	Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS	
System operacyjny do zaoferowanego serwera wraz z 10 licencjami dostępowymi na użytkownika	**Licencja:** 1) Wykonawca dostarczy licencje i oprogramowanie w formie elektronicznej lub umożliwi Zamawiającemu ich pobranie ze strony producenta. 2) Windows Server 2022 lub równoważny (warunki równoważności podane poniżej) w wersji pozwalającej na uruchomienie nie mniej niż 2 szt. systemów wirtualnych Windows Server 2022 na zaproponowanym sprzęcie. 3) Zamawiający wymaga, aby licencja była zgodną z oferowaną w serwerach ilością procesorów i rdzeni oraz z zaproponowaną ilością możliwych do uruchomienia na nich systemów wirtualnych Windows Server 2022. 4) Wieczysta. 5) Wersja polskojęzyczna. 6) OEM, Zamawiający dopuszcza licencje typu ROK. Licencje na zamawiany serwerowy system operacyjny muszą być bezterminowe. 8) Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego spełniająca jednocześnie poniższe: a) Minimalna obsługiwana pamięć RAM przynajmniej 16GB, b) Maksymalna obsługiwana pamięć RAM nie mniej niż 24TB. 9) Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym.	

	10) W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego. 11) Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. 12) Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu. 13) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6. 14) Zawarta funkcjonalność szyfrowania dysków. 15) Dostępna wbudowana funkcjonalność umożliwiająca uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera. 16) Praca w roli klienta domeny Microsoft Active Directory. 17) Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022. 18) Zawarta możliwość uruchomienia roli serwera DHCP. 19) Zawarta możliwość uruchomienia roli serwera DNS. 20) Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP). 21) Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 22) Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). 24) Obsługa PowerShell 6.0. 25) Obsługa certyfikatow w AD. 26) Z uwagi na szeroki zakres funkcjonalny planowanego wdrożenia na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga, aby zaoferowane licencje, umożliwiały wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania. 27) Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania (umożliwia downgrading). 28) Wymagane jest, aby podstawowe informacje na temat instalacji i użytkowania oprogramowania były dostępne na witrynie producenta. **Warunki równoważności**: 1) W przypadku zaoferowania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że zaoferowane produkty spełniają wszystkie wymagania i warunki określone w OPZ, w szczególności w zakresie:	

a) spełnienia warunków niezbędnych do realizacji założonego

zastosowania w zakresie zaoferowanych produktów równoważnych w każdym aspekcie, które nie mogą być gorsze niż dla produktów

wymienionych w OPZ,

c) warunków licencji / sublicencji / subskrypcji zaoferowanych produktów równoważnych w każdym aspekcie, które nie mogą być gorsze niż dla produktów wymienionych w OPZ,

d) funkcjonalności zaoferowanych produktów równoważnych, które nie mogą być ograniczone i gorsze względem funkcjonalności produktów wymienionych w OPZ,

e) zakresu kompatybilności i współdziałania zaoferowanych produktów równoważnych ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego, który nie może być gorszy niż dla produktów wymienionych w OPZ,

f) poziomu zakłóceń pracy środowiska systemowo-programowego

Zamawiającego spowodowanego wykorzystaniem zaoferowanych

produktów równoważnych, który nie może być większy niż w

przypadku produktów wymienionych w OPZ,

g) poziomu współpracy zaoferowanych produktów równoważnych z

systemami Zamawiającego, który nie może być gorszy od tego jaki

zapewniają produkty wymienione w OPZ,

h) zapewnienia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności zaoferowanych produktów równoważnych z produktami wymienionymi w OPZ,

i) warunków i zakresu usług gwarancji, asysty technicznej i konserwacji zaoferowanych produktów równoważnych, które nie mogą być gorsze niż dla produktów wymienionych w OPZ,

j) obsługi przez zaoferowane produkty równoważne języków interfejsu, w ilości i rodzaju nie mniejszych niż oferują produkty wymienione w OPZ,

k) wymagań sprzętowych dla zaoferowanych produktów równoważnych, które nie mogą być wyższe niż dla produktów wymienionych w OPZ,

l) dostępności wersji bitowych (32, 64) zaoferowanych produktów

równoważnych, która nie może być mniejsza niż dla produktów

wymienionych w OPZ.

2) W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego.

3) W przypadku zaoferowania przez Wykonawcę oprogramowania

równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.

4) W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie

	współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego. 5) Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania. 6) Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.	
Waga	maximum: 38.8kg	
Gwarancja	Serwer powinien posiadać 60 miesięcy gwarancji producenta on-site z czasem reakcji NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego. Dyski zainstalowane w serwerze muszą mieć taką samą gwarancję jak serwer. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.	
Certyfikat	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 Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.	
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). 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 cykle. 15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock"). 16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami. 17. 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. 18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie. 19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia. 20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu. 21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych 22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS. 23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego. 24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii). 25. 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.

26. 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.

27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,

28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.

29. 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.

30. 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).

31. 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.

32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.

33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych

34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.

35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.

36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.

37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.

38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.

39. System musi pozwalać na automatyczne aktualizacje oprogramowania.

40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.

41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.

42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.

43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.

44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.

45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.

46. System musi pozwalać na gradację uprawnień administratorów - umożliwia 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.

47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.

48. 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.

49. 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.

50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.

51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,

53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).

54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.

55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny

56. 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).

57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami 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.

	58. Możliwość generowania raportów dobowych w oparciu o harmonogram 59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski) 60. 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) 61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP. 62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)	
Wspierane systemy	Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: Alpine 3.10+, Debian: 9+, Ubuntu: 16.04+, Fedora: 29+, centOS: 7+, RHEL: 6+, openSUSE: 15+, SUSE Enterprise Linux(SLES): 12 SP2+, macOS: 10.13+, Windows: 7, 8.1, 10, 11 Windows Server: 2008 R2+, Środowisk wirtualnych: Hyper-V 2016+, VMware: 6.7+. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: Debian: 9+ Ubuntu: 16.04+ Fedora: 29+ centOS: 7+	

	RHEL: 6+ openSUSE: 15+ SUSE Enterprise Linux (SLES): 12 SP2+ Windows Client: 7, 8.1, 10 ,11 Windows Server: 2012 R2+,	
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 scalania danych. 7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. 8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. 9. 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. 10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych. 11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V. 12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK). 13. 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.	

	14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).	
Środowiska wirtualne	1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów. 2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie 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 wraz z metadanymi 5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe. 6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git. 7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium. 8. System musi umożliwiać zabezpieczenie środowisk Jira 9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska	

	lokalnego. 10. System musi umożliwiać zabezpieczenie środowisk Jira	
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 bezpośrednio z poziomu interfejsu zarządzania w formie czatu. 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 w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk. 7. Licencje powinny być dostępne w opcji wieczystej. 8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. 24 miesięcy 9. Sposób licencjonowania opiera się na: - ilości serwerów/endpointów - dla fizycznych urządzeń, - ilości socketów w hostach - dla środowisk wirtualnych, - ilość repozytoriów - dla GIT, - Ilość serwerów wirtualnych (licencjonowanie opcjonalne). 10. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej: - 50 stacji roboczych, - 1 serwer wirtualny, - Nielimitowanej ilości maszyn wirtualnych w obrębie 1 fizycznego serwera stanowiących podstawy do wirtualizacji (łącznie 2 sockety),	
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 menedżera 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. 4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego	

	awaria sparaliżowały by działanie Systemu. System nie może posiadać pojedynczego punktu awarii. 5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.	

....

miejscowość i data /Podpis i pieczęć osoby upoważnionej