**Zał. Nr 1 OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Doposażenie Serwerowni - Serwer**

**Producent: …………………………………….**

**Model: …………………………………….**

**Ilość: 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **Procesor** | Zainstalowane jeden procesory min. 10-rdzeniowy, min. 2.1 GHz (Turbo Speed min. 3.3 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 23 000 punktów w teście Average CPU Mark dostępnym na stronie <https://www.cpubenchmark.net/>. |  |
| **RAM** | 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling |  |
| **Gniazda PCI** | - minimum cztery sloty PCIe z czego przynajmniej trzy generacji 4  |  |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| **Dyski twarde** | Możliwość instalacji dysków SAS, SATA, SSDZainstalowane: * 4 dyski SSD o pojemności min. 1,92 TB, Hot-Plug,
* 4 dyski o pojemności min. 10TB, Hot-Plug

Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |  |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  |  |
| **System operacyjny/System wirtualizacji** | System operacyjny do serwera administracji i monitorowania oraz zarządzania środowiskiem zwirtualizowanym (wymagana jest zgodność z oprogramowaniem już wykorzystywanym u Zamawiającego, m.in. w zakresie współpracy z Active Directory). System do serwerów powinien mieć możliwość postawienia 2 maszyn wirtualnych.RównoważnośćZamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilne w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby ZamawiającegoDodatkowo wykonawca dostarczy 20 szt. licencji dostępowych na urządzenie dla serwerowego systemu operacyjnego |  |
| **Wbudowane porty** | Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0, |  |
| **Napęd Optyczny** | Wbudowany napęd DVD +/- RW SATA |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Zasilacze** | Redundantne, Hot-Plug min. 800W każdy |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
 |  |
| **Diagnostyka** | Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* 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 autentykacje 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 dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
 |  |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. |  |
| **Warunki gwarancji** | 3 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty.Możliwość rozszerzenia gwarancji przez producenta do 7 lat.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |

1. **Doposażenie Serwerowni - serwerowy system operacyjny**

**Producent: …………………………………….**

**Model: …………………………………….**

**Ilość: 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Serwerowy system operacyjny musi zostać dostarczony w najnowszej wersji producenta oprogramowania. System operacyjny musi spełniać następujące wymogi: licencja musi uprawniać do wykorzystania min. 16 rdzeni fizycznych procesorów zamontowanych w serwerów oraz uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji; Możliwość wykorzystania, co najmniej 120 logicznych procesorów oraz co najmniej 3 TB pamięci RAM w środowisku fizycznym; Możliwość wykorzystywania 32 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 32 TB przez każdy wirtualny serwerowy system operacyjny; Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci; Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy; Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy; Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego; Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji; Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET; Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów; Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play); Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu; Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet; Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath); Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego; Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |  |

1. **Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania**

**Ilość: 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Wykonawca w ramach usługi wykona:1. Segmentacji sieci fizycznej na podsieci VLAN, uwzględniając dobre praktyki. Wydzielinie VLAN-ów:a. Zarządzaniab. Serwerówc. Stacji Roboczychd. Drukarek i urządzeń peryferyjnyche. Zarządzania kryzysowegof. Gości2. Montaż i instalacja zakupionego serwera w sieci zamawiającego, instalacja i konfiguracja środowiska Windows Server HyperV:a. Instalacja i konfiguracja serwera HyperVb. Instalacja i konfiguracja maszyny wirtualnej - serwera Kontrolera domeny Active Directoryi. Uruchomieni usługi Active directory certificate servicesii. Uruchomieni usługi NPS1. Instalacja i konfiguracji stacji roboczych do autoryzacji po protokole 802.1x (autoryzacja certyfikatami)iii. Uruchomieni usługi LAPSiv. Instalacja i konfiguracja 20 stacji roboczych wraz konfiguracją oprogramowani i podłączeniem do Domeny Active Directory1. Instalacja i konfiguracja aplikacji używanych przez Zamawiającego na stacjach roboczych.c. Instalacja i konfiguracja maszyny wirtualnej - serwera aplikacji i baz danychi. Uruchomieni usługi MS SQL Serwerii. Uruchomieni usługi Firebird Serweriii. Uruchomieni usługi WSUSiv. Uruchomieni usługi Serwera Wydruku1. Konfiguracja drukarek oraz urządzeń wielofunkcyjnych w usłudze serwera wydruku, podłączeni do sieci LAN instalacja na stacjach roboczych. Instalacja skanowania do sieci i email.v. Uruchomieni usługi Plików / Udziałów sieciowychvi. Uruchomieni usługi Folder Redirection – przekierowanie katalogów z profilu użytkownikavii. Uruchomieni usługi FSRMviii. Migracja aplikacji używanych przez Zamawiającego na serwer aplikacji i baz danych1. Płatnik ZUS2. Bestia JST3. Progman Finanse4. Progman Rozrachunki5. Progman Zbiorczy VAT6. Progman Wyposarzenie7. Legislator8. Axence Nvision9. Kadry i Płace 10. Groszek Auta11. Groszek Kasa12. Groszek Kszob13. Groszek Oplok14. Groszek Podatki15. Groszek Przelewy16. Groszek UPKd. Instalacja i konfiguracja maszyny wirtualnej - serwera terminali i. Konfiguracja połączenia VPN do serwera terminali.ii. Konfiguracja połączeń VPN na komputerach przenośnych zamawiającegoiii. Instalacja i konfiguracja aplikacji używanych przez Zamawiającego na serwerze terminali.e. Instalacja i konfiguracja maszyny wirtualnej – serwera do zbierania logów z urządzeń sieciowych (Greylog)f. Instalacja i konfiguracja maszyny wirtualnej – serwera kontrolera sieci WiFI- UniFIg. Instalacja i konfiguracja maszyny wirtualnej – do zbierania kopii zapasowych z urządzeń sieciowych (Oxidized)h. Instalacja i konfiguracja maszyny wirtualnej – serwera do zbierania logów z bramy UTM (FortiAnalyzer)i. Instalacja i konfiguracja maszyny wirtualnej - serwera konsoli Antywirusowej ESETj. Instalacja i konfiguracja maszyny wirtualnej - serwera dla środowiska do wykonywania kopii zapasowych w oparciu o zakupione przez Zamawiającego licencję Veeam Universal License Essential (lub równoważne). Obejmuje to:i. Wdrożenie polityk backupowych w środowisku Zamawiającego.ii. Zaprojektowanie w współpracy z Zamawiającym harmonogramu wykonywania kopii, z uwzględnieniem środowiska Zamawiającego.iii. Instalację oprogramowania w środowisku Zamawiającego.iv. Implementację harmonogramu wykonywania kopii w zainstalowanym oprogramowaniu.v. Wykonanie testowych kopii środowiska Hyper-V, wraz z weryfikacją poprawności ich wykonania.vi. Testy odtworzenia danych środowiska Hyper-V.k. Konfiguracja zakupionego oprogramowaniu backupu do obsługi napędu taśmowego oraz wdrożenie polityk backupowych w uwzględniających kopie zapasowe na ten napęd.l. Konfiguracja zakupionego oprogramowaniu bakupu do obsługi macierzy dyskowych NAS oraz wdrożenie polityk backupowych w uwzględniających kopie zapasowe na te macierze.m. Instalacja i konfiguracja chmurowej usługi kopii zapasowych oraz wdrożenie polityk backupowych w oprogramowaniu do backupu uwzględniających kopie zapasowe do chmury. |  |

1. **Chmura obliczeniowa dla JST**

**Producent: …………………………………….**

**Model: …………………………………….**

**Ilość: 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Wykonawca zapewni przestrzeń w chmurze obliczeniowej o pojemności magazynu danych minimum 1TB. Usługa dostępna na min. 1 ROK do celów przechowywania kopii zapasowych.Usługa musi zapewnić:1. Usługa musi zapewniać współpracę z zakupionym przez zamawiającego oprogramowaniem do backupu2. Odciążanie lokalnej kopii zapasowej, rozwiązanie do tworzenia kopii zapasowych zasobów lokalnych w chmurze. 3. Krótkoterminowe i długoterminowe kopie zapasowe bez konieczności wdrażania złożonych lokalnych rozwiązań do wykonywania kopii zapasowych.4. Tworzenie kopii zapasowych maszyn wirtualnych 5. Kopie zapasowe są przechowywane w magazynie z wbudowanymi funkcjami zarządzania punktami odzyskiwania. 6. Skalowanie - używa dostępnej mocy i nieograniczonej skali chmury do zapewniania wysokiej dostępności, bez narzutu na konserwację lub monitorowanie.7. Pobieranie nieograniczonego transferu danych: Usługa nie ogranicza ilości przesyłanych danych przychodzących lub wychodzących ani opłat za transferowane dane.8. Zabezpieczanie danych: Usługa zapewnia rozwiązania do zabezpieczania danych przesyłanych i magazynowanych.9. Scentralizowane monitorowanie i zarządzanie.10. Kopia zapasowa spójna na poziomie aplikacji - punkt odzyskiwania zawiera wszystkie dane wymagane do przywrócenia kopii zapasowej, co zapewnia, że do przywrócenia danych nie są wymagane dodatkowe poprawki. 11. Wiele opcji magazynowania - trzy typy replikacji, aby zapewnić wysoką dostępność magazynu/danych. |  |
| **Zarządzanie danymi kopii zapasowych na dużą skalę** | Zarządzanie całym obszarem kopii zapasowych i monitorowania z centralnej konsoli za pomocą Centrum kopii zapasowych.Zachowanie zgodność, wymuszając tworzenie kopii zapasowych na dużą skalę.Kontrola i analiza danychkopii zapasowych przy użyciu danych historycznych i wzorców przedstawionych w Raportach kopii zapasowych.Interfejs API do automatyzacji zasad tworzenia kopii zapasowych i konfiguracji zabezpieczeń.Eksport danych kopii zapasowych w chmurze do własnych systemów monitorowania w bezpieczny i wydajny sposób. |  |
| **Zabezpieczanie kopii zapasowych** | Przydzielenie użytkownikom szczegółowego dostępu do konkretnych operacji tworzenia kopii zapasowych przy użyciu kontroli dostępu opartej na rolach (RBAC).Zapobieganie przypadkowej utracie danych, przechowując kopie zapasowe przez 14 dni po usunięciu z usuwaniem nietrwałym.Ochrona danych przed atakami z użyciem oprogramowania wymuszającego okup, włączając uwierzytelnianie wielu użytkowników jako dodatkową warstwę autoryzacji dla operacji krytycznych.Kontrola sposóbu ochrony danych i uzyskiwania do nich dostępu za pomocą kluczy zarządzanych przez klienta, które używają 256-bitowe szyfrowanie AES.Bezpieczny transfer kopii zapasowych do magazynu usługi z prywatnymi punktami końcowymi.Zapewnienie dostępność magazynu strefowo-geograficznie nadmiarowego oraz możliwość przywracania kopii zapasowych ze sparowanego regionu w dowolnym momencie. |  |
| **Ochrona zróżnicowanego zestawu obciążeń** | Wykonanie kopii zapasowej całej infrastruktury, baz danych, i obciążenia magazynu z centralnej lokalizacji.Spójność na poziomie aplikacji migawki usługi Virtual Machines działające zarówno w systemach Windows, jak i Linux.Generuj migawki usługi Azure Disks.Zabezpieczenie przed utratą dane. |  |

1. **Szkolenia dla urzędników w zakresie cyberbezpieczeństwa**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Szkolenia dla min. 20 pracowników Zamawiającego w zakresie cyberbezpieczeństwa.1. Miejsce szkolenia: Urząd Gminy w Dzierzążni – (szkolenie stacjonarne)2. Wielkość grup: Grupy nie mogą przekraczać 4 osób. 3. Czas szkolenia: a. Szkolenie może odbywać się w godzinach 10-14, b. Każda grupa innego dnia tygodnia. c. Łącznie w ciągu 5 dni roboczych.4. W szkoleniach uczestniczyć będą pracownicy Zamawiającego.5. Każdy uczestnik otrzyma dokument poświadczający ukończenie szkolenia.6. Szkolenia muszą zostać przeprowadzone w języku polskim.7. Szkolenie odbędzie się w formie prezentacji, demonstracji, pokazów itp. z wykorzystaniem dedykowanych materiałów szkoleniowych.8. Zakres merytoryczny szkolenia musi obejmować minimalnie tematy wyszczególnione poniżej:a. Zagrożenia i rozwiązania, czyli jak zapewnić sobie bezpieczeństwo na prywatnej poczcie, Facebooku, Twitterze, Instagramie i innych popularnych portalach.b. Klucze/hasła dostępowe – jak stosować w praktyce.c. Typowe ataki wyłudzające pieniądze.d. Przykłady ataków w mediach społecznościowych.e. Ataki z wykorzystaniem socjotechnikif. Bezpieczeństwo Poczty e-mailg. Bezpieczeństwo przeglądarek internetowychh. Ataki za pośrednictwem telefonui. Zagrożenia związane w urządzeniami mobilnymij. Zagrożenia związane z sieciami WIFI |  |

1. **Zakup specjalistycznego oprogramowania – oprogramowanie do backupu**

**Producent: …………………………………….**

**Wersja: …………………………………….**

**Ilość: 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Uniwersalna wieczysta licencja oprogramowania do backupu, umożliwiającego wykonywanie kopii zapasowych serwerów – 15 szt.1. 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 4,5.2. Oprogramowanie musi współpracować z infrastrukturą Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, 3. Oprogramowanie musi współpracować z serwerami zarządzanymi przez Microsoft Hyper-V oraz pojedynczymi hostami.4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez Hyper-V.5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.6. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.7. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.8. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental).9. 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.10. 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.11. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.13. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.14. 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.15. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. 16. Dostawa oprogramowania do archiwizacji m.in. maszyn wirtualnych Hyper-V z możliwością automatycznego odtworzenia całej maszyny wirtualnej z kopii oraz z kopii już obecnie posiadanych utworzonych przez Zamawiającego, zgodnego z obecnie posiadanym przez Zamawiającego oprogramowaniem Veeam Backup & Replication. |  |

1. **Zakup specjalistycznego oprogramowania II**

**Producent: …………………………………….**

**Wersja: …………………………………….**

**Ilość: 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowany parametr** |
| **Opis** | Dostawa licencji oprogramowania(lub aktualizacji) systemu zarządzania i monitoringiem sieci składającego się z następujących modułów:1. Network
* skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
* interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
* jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
* serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
* liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
* możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca)
* działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
* liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
* kompilator plików MIB
* obsługa pułapek SNMP
* routery i switche: mapowanie portów
* obsługa komunikatów syslog
* alarmy zdarzenie - akcja
* powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)
* raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)
1. Inventory
* audyt inwentaryzacji sprzętu i oprogramowania
* wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
* zdalny dostęp do managera plików z możliwością usuwania plików użytkownika
* informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej
* szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
* zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI
* alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
* lista kluczy oprogramowania Microsoft
* aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR
* możliwość archiwizacji i porównywania audytów
* monitorowanie harmonogramu zadań Windows
1. Users
* minimalizacja zjawiska cyberslackingu i zwiększenie wydajności pracowników
* redukcja kosztów wydruku
* blokowanie stron WWW
* blokowanie uruchamianych aplikacji
* monitorowanie wiadomości e-mail (nagłówki) - antyphishing
* szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)
* użytkowane aplikacje (aktywnie i nieaktywnie)
* odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
* audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
* użycie łącza: generowany przez użytkowników ruch sieciowy
* statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
* zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)
* blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE
* zarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników)
1. HelpDesk
* dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę
* dwa tryby widoku - jasny i ciemny
* planowanie zastępstw w przydzielaniu zgłoszeń
* rozbudowany system raportów
* powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym
* baza zgłoszeń z rozbudowaną wyszukiwarką
* baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube
* przejrzysty i intuicyjny interfejs webowy
* wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych
* komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu
* zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury
* dwukierunkowa wymiana plików
* zarządzanie procesami Windows z poziomu okna informacji o urządzeniu
* zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)
* procesowanie zgłoszeń z wiadomości e-mail
* integracja bazy użytkowników z Active Directory
* zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont)
* zdalna edycja rejestru na komputerach
1. DataGuard
* zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami
* informacje o urządzeniach podłączonych do danego komputera
* lista wszystkich urządzeń podłączonych do komputerów w sieci
* audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych
* zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników
* centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory
* integracja bazy użytkowników i grup z Active Directory
* alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym

Serwisem producenta oprogramowania na min. 12 miesięcyIlość stacji roboczych: min. 37  |  |