*Załącznik nr 1 do SWZ – Szczegółowy opis przedmiotu zamówienia*

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Serwer – 2 szt.

|  |  |
| --- | --- |
| **Parametr**  | **Charakterystyka (wymagania minimalne)**  |
| **Obudowa**  | Obudowa Rack o wysokości min. 2U umożliwiającą instalację min. 16 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  |
| **Płyta główna**  | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  |
| **Chipset**  | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych  |
| **Procesor**  | Zainstalowany jeden procesor min. szesnasto-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 334 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Dla oferowanego serwera. |
| **RAM**  | Min. 256GB DDR4 RDIMM 5600MT/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**  | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) |
| **Interfejsy sieciowe/FC/SAS**  | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.Dwa interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 nie zajmujące slotów PCIe. Dodatkowe zainstalowane:- jedna karta czteroportowa 1Gb Ethernet w standardzie BaseT.- jedna karta dwuportowa FC 32Gb/s |
| **Dyski twarde**  | Zainstalowane 2 x 480GB SSD SATA, DWPD min. 3 skonfigurowane w RAID 1.Możliwość instalacji dwóch dysków hot-swap M.2 NVMe o pojemności min. 960GB z możliwością konfiguracji RAID 1.  |
| **Wbudowane porty**  | min. port USB 2.0 oraz port USB 3.0, port VGA, |
| **Video**  | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900  |
| **Wentylatory**  | Redundantne  |
| **Zasilacze**  | Min. dwa zasilacze Hot-Plug maksymalnie 700W Titanium.  |
| **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 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serweraMożliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.Możliwość integracji z RSA SecurID |
| **Karta Zarządzania**  | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
* zdalny dostęp do graficznego interfejsu Web karty zarządzającej
* 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 SNMP; IPMI2.0, VLAN tagging, SSH
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
* integracja z Active Directory
* możliwość obsługi przez trzech administratorów jednocześnie
* Wsparcie dla automatycznej rejestracji DNS
* wsparcie dla LLDP
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
* możliwość podłączenia lokalnego poprzez złącze RS-232.
* możliwość zarządzania bezpośredniego poprzez złącze microUSB lub USB-A lub USB-C - umieszczone na froncie obudowy.
* Monitorowanie zużycia dysków SSD
* możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
* Automatyczne zgłaszanie alertów do centrum serwisowego producenta
* Automatyczne update firmware dla wszystkich komponentów serwera
* Możliwość przywrócenia poprzednich wersji firmware
* Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON
* Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych
* Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.
* Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera
* Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI.
* Karta powinna umożliwiać rozszerzenie funkcjonalności o:
* możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych
* kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania
* Automatyczne odświeżanie certyfikatów SSL
* możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej
* możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień
* możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera
* możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer
* możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe
* monitorowanie przepływu powietrza na bieżąco
 |
| **Oprogramowanie do zarządzania** |  Możliwość zainstalowania oporgrmowania producenta do zarządznia, spełniające poniższe wymagania: * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
* integracja z Active Directory
* Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
* Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
* Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
* Szczegółowy opis wykrytych systemów oraz ich komponentów
* Możliwość eksportu raportu do CSV, HTML, XLS, PDF
* Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu.
* Grupowanie urządzeń w oparciu o kryteria użytkownika
* Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
* Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
* Szybki podgląd stanu środowiska
* Podsumowanie stanu dla każdego urządzenia
* Szczegółowy status urządzenia/elementu/komponentu
* Generowanie alertów przy zmianie stanu urządzenia.
* Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
* Integracja z service desk producenta dostarczonej platformy sprzętowej
* Możliwość przejęcia zdalnego pulpitu
* Możliwość podmontowania wirtualnego napędu
* Kreator umożliwiający dostosowanie akcji dla wybranych alertów
* Możliwość importu plików MIB
* Przesyłanie alertów „as-is” do innych konsol firm trzecich
* Możliwość definiowania ról administratorów
* Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
* Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
* Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
* Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
* Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
* Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności.
* Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile
* Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
* Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
* Zdalne uruchamianie diagnostyki serwera.
* Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym.
* Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
 |
| **Komponenty dodatkowe** | 4 x moduł nadawczo-odbiorczy 10GbE SFP+ SR |
| **Certyfikaty**  | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.  |
| **Normy Środowiskowe**  |  Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku *-****Wykonawca złoży dokument potwierdzający spełnianie*wymogu*.*** Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera**(wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr *-****Wykonawca złoży dokument potwierdzający spełnianie*wymogu*.***  |
| **Warunki gwarancji**  | Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***wykonawcy / producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę. 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. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowyych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii . Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych |
| **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. Oprogramowanie do backupu – 10 szt. maszyn wirtualnych

|  |  |
| --- | --- |
| **Parametr**  | **Charakterystyka (wymagania minimalne)**  |
| Wymagania podstawowe | Oferowane rozwiązanie musi znaleźć się w czołówce raportu Gartner Magic Quadrant for Data Center Backup and Reocvery Solutions. Dodatkowo musi znajdować się na liście referencyjnej Gartner https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions z minimalnym wymogiem 150 referencji i minimalnym wynikiem 4,5 . |
| Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
| Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. |
|  Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. |
| 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. |
| Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
| Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
|  Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) |
| 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 |
| 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. |
| 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. |
| Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Google Cloud Storage, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. |
| Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
| Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. |
| Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) |
| Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
| Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
| Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
| Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
| Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
| Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) |
| Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
| Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
| Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) |
| Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
| Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
| Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
| 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 |
| Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru |
| Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora |
| 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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, INFINIDAT, Pure Storage. |
| Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
| Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn |
| Oprogramowanie musi posiadać wsparcie dla NDMP |
| Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
| Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |
| Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |
| 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. |
| Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability) |
| Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
| 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. |
| Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
| Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
| Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
| Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| 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. |
| Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| 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 |
| Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
| Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
| Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
| Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
| Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs; BSD: UFS, UFS2; Solaris: ZFS, UFS; Mac: HFS, HFS+; Windows: NTFS, FAT, FAT32, ReFS; Novell OES: NSS. |
| Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. |
| Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
| Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. |
| Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), |
| Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych |
| Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska |
| Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych |
| Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. |
| 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. |
| Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
| Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA |
| Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. |
|  Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |
| 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 |
| Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere |
| 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. |
| Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| Monitoring | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
| System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware |
| System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
| System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
| System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
| System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
| System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
| System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
| System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
| System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
| System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
| System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
| System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
| System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |
| System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |

1. Licencje oprogramowania antywirusowego z funkcją XDR (endpoint) szt – 90 szt.

|  |  |
| --- | --- |
| **Parametr**  | **Charakterystyka (wymagania minimalne)**  |
|  | System musi umożliwiać administratorom identyfikację danych dotyczących incydentów bezpieczeństwa, oferując analizę obejmującą charakterystykę ataku, metodę jego inicjacji, konsekwencje oraz strategie odpowiedzi. |
| Kompatybilność | System jest kompatybilny z istniejącymi infrastrukturami IT i może być zintegrowany z różnymi platformami operacyjnymi. |
| Integracja danych bezpieczeństwa | Umożliwia zbieranie i analizę danych z oprogramowania antywirusowego, workloadów, serwerów, firewalli, ZTNA, NDR, systemów SIEM, smartphonów, e-maili oraz chmur. |
| Wykrywanie zagrożeń | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Używać zaawansowanych technik uczenia maszynowego i algorytmów sztucznej inteligencji do wykrywania nowych i rozwijających się zagrożeń. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanego wcześniej złośliwego oprogramowania, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. Wybitnie wysoka skuteczność powinna być potwierdzona w testach organizacji takich jak: Gartner, SE Labs, MITRE itd. |
| Skalowalność | Rozwiązanie oferuje wysoką skalowalność, zapewniając efektywność operacyjną w środowiskach o różnym stopniu złożoności i rozmiaru. |
| Dostęp | System musi być zarządzalny zdalnie za pomocą konsoli chmurowej z każdego miejsca na świecie. Rozwiązanie musi pozwalać Administratorom na zdalny i bezpieczny dostęp do urządzeń przy użyciu konsoli. |
| Automatyzacja odpowiedzi | Automatyzuje odpowiedzi na incydenty, zmniejszając czas reakcji i obciążenie zespołów IT. |
| Analiza zagrożeń w chmurze | Wykorzystuje globalne zasoby producenta do ciągłej analizy zagrożeń i aktualizacji systemu w czasie rzeczywistym |
| Active Directory | Rozwiązanie musi zapewniać integrację z Active Directory oraz LDAP (usługą katalogową, hierarchiczna baza danych) |
| Klasyfikacja plików i aplikacji | Umiejętność klasyfikowania jako złośliwe, potencjalnie niechciane, lub niegroźne oraz możliwość ich zablokowania. |
| Blokowanie aplikacji | Możliwość blokowania aplikacji niepożądanych w miejscu pracy |
| URL filtering | Usługa pozwalająca na kontrolę dostępu do wybranych stron internetowych oraz stron oddanej kategorii i tematyce. |
| Wykorzystanie telemetrii stron trzecich | Możliwość przyjmowania alertów z urządzeń i aplikacji innych producentów, odpowiednia ich filtracja i korelacja w celu wzbogaceniu widoczności. |
| Bezpieczeństwo danych | Wdrożenie silnych mechanizmów szyfrowania i autentykacji, zapewniających ochronę danych przed nieautoryzowanym dostępem. W tym wsparcie TLS 1.3. |
| Przechowywanie danych z XDR | Min. 90 dni zarówno na endpoincie, jak i w chmurze. |
| AMSI | Ochrona przed szkodliwym kodem (np. skrypty PowerShell) |
| IPS (Intrusion Prevention System – system wykrywania i zapobiegania włamaniom) | System musi być zdolny do monitorowania ruchu poprzez inspekcję pakietów na poziomie endpointa (komputera/stacji roboczej z zainstalowanym oprogramowaniem antywirusowym). |
| DLP | Wsparcie dla DLP (Data Loss Prevention - system zapobiegania utracie danych lub system zapobiegania wyciekom danych) oraz możliwość tworzenia polityk DLP. |
| Blokada nośników | Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pendrive, urządzeń Bluetooth, modemów. |
| Dashboarding | Musi posiadać wysoce modyfikowalny dashboard (tablice rozdzielczą/zarzadczą) z biblioteką widżetów pozwalających na intuicyjną analizę zagrożeń. Rozwiązanie musi pozwalać na skonfigurowanie i możliwość zapisu kilku wcześniej stworzonych dashboardów. |
| Kwarantanna stacji roboczej | Umożliwia automatyczne bądź manualne odizolowanie zainfekowanego urządzenia od sieci, blokując wszystkie połączenia przychodzące i wychodzące. Po zainicjowaniu, jedynie administrator ma dostęp do stacji z poziomu konsoli rozwiązania. |
| Funkcjonalność bez dostępu do Internetu | Rozwiązanie musi pozwalać na skanowanie w czasie rzeczywistym w trybie offline. |
| Przejrzystość i łatwość obsługi | Rozwiązanie musi być przejrzyste i nie może być skomplikowane w użyciu. Potrzeba użycia kilku konsol do obsługi całego systemu jest niedopuszczalna. |
| Unifikacja | Rozwiązanie musi w całości pochodzić od jednego producenta. Użycie połączenia kilku produktów w celu spełnienia warunków specyfikacji technicznej jest zabronione. |
| Powiadomienia | System musi posiadać funkcjonalność powiadomienia administratora w chwili utworzenia bądź modyfikacji dochodzenia przy użycia wiadomości e-mail. |
| Ochrona przed dezinstalacją | System musi implementować mechanizmy zabezpieczające przed nieautoryzowanym odinstalowaniem oprogramowania, nawet przez osoby posiadające uprawnienia administratora lokalnego na danym komputerze. Realizacja tego zabezpieczenia powinna wymagać użycia dodatkowego hasła. Ponadto, istotna jest możliwość modyfikacji tego hasła oraz dezaktywacji mechanizmu ochrony bezpośrednio z centralnej konsoli zarządzającej. |
| Ochrona przed kradzieżą haseł | Musi zapewniać ochronę przed kradzieżą haseł z pamięci podręcznej. |
| Ochrona przed eskalacją uprawnień | Musi posiadać mechanizm zabezpieczający przed podniesieniem uprawnień. |
| Ochrona przed zaszyfrowaniem danych | Rozwiązanie musi posiadać mechanizm zabezpieczający przed atakami Ransomware ( złośliwego oprogramowania, które blokuje pliki lub urządzenie użytkownika, a następnie żąda anonimowej płatności online w celu przywrócenia dostępu). |
| Ochrona przed złośliwym oprogramowaniem | Rozwiązanie musi posiadać mechanizm ochrony przed złośliwym oprogramowaniem typu Rootkit (infekującego jądro i usuwającego ukrywane programy z listy procesów oraz plików zwracanych do programów) i Bootkit (złośliwe oprogramowanie uruchomiane w trakcie startu systemu, zaprojektowanego w celu uzyskania niskopoziomowej kontroli nad komputerem bez wiedzy właściciela). |
| Analiza behawioralna użytkownika | Analiza behawioralna użytkownika w celu rozpoznania zagrożeń. |
| White & Black Listing | Możliwość skonfigurowania białej i czarnej listy usług w celu zawężenia liczby dostępnych usług. |
| Zgodność i certyfikaty | System jest zgodny z normami i standardami branżowymi, takimi jak ISO 27001 i ramy NIST. |
| Uwierzytelnienie wieloskładnikowe | Rozwiązanie musi posiadać możliwość zastosowania MFA dla administratorów logujących się do systemu/konsoli chmurowej. Wsparcie Authy, MS Authenticator, Google Authenticator, wiadomości mailowej i SMS. |
| Funkcje dodatkowe | Funkcja zabezpieczająca przed ponownym uruchomieniem urządzeń w trybie bezpiecznym. Funkcja pozwalająca na wykrycie ataku hakerskiego prowadzonego w czasie rzeczywistym, poprzez rozpoznanie powszechnie stosowanych narzędzi hakerskich (toolkitów) i potencjalnie szkodliwych zachowań oraz umiejętność aktywnego blokowania ataku w przypadku jego wykrycia. Funkcja umożliwiająca sprawdzenie stanu zdrowia konta użytkownika, pozwalająca na łatwe zauważenie problemów związanych z bezpieczeństwem systemu. System musi posiadać funkcję analizy zagrożeń na wykresie. Funkcja pozwalająca na inspekcję danych przesyłanych przez SSL/TLS. Funkcja blokująca pobieranie szkodliwych i niepożądanych treści.  |
| Szyfrowanie | Funkcja pozwalająca na zaszyfrowanie oraz odszyfrowanie dysku urządzenia oraz wymianę haseł przez konsolę administratora/chmurową |
| Polityki | Możliwość tworzenia polityk dla użytkowników i urządzeń. Funkcja automatycznego wyłączenia polityki według harmonogramu. |
| Windows Firewall | Rozwiązanie musi poprawnie współpracować z Windows Firewall. |
| Archiwizacja | Rozwiązanie musi być w stanie zapisać historię i analizę przeprowadzonego ataku oraz wyeksportowanie go formatów takich jak SQLite, czy JSON. |
| Wyszukiwanie | Rozwiązanie musi pozwalać na łatwe wyszukiwanie treści przy użyciu zapytań SQL |
| Wymagania systemowe hardware | Agent nie może używać dużej ilości zasobów stacji roboczej |
| Rozwiązanie musi działać na systemach operacyjnych  | Windows 11 & 10 (64-bit), Windows Server 2012 i nowsze, Mac OS 12 i nowsze,  |
| Linux: Amazon Linux 2, Amazon Linux 2023, CentOS 7 (3.10.0-1062 lub późniejsze), CentOS Minimal, CentOS Stream, Debian 10, Debian 11, Debian 12, Miracle Linux 8, Oracle 7 (UEK 4.14 lub późniejsze, RHCK 3.10.0-1062 lub późniejsze), Oracle 8, Oracle 9, RHEL 7 (3.10.0-1062 lub późniejsze), RHEL 8, RHEL 9, SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15, Ubuntu 18.04 (LTS) (4.15 lub późniejsze), Ubuntu 20.04 (LTS), Ubuntu 22.04 (LTS), Ubuntu Minimal |
| Rozwiązanie powinno także oferować możliwość rozszerzenia licencji o wersje mobilne działające na systemach: Android, iOS. |
| Wsparcie i aktualizacje | Wsparcie techniczne producenta na czas trwania licencji. Regularne aktualizacje oprogramowania, w tym poprawki bezpieczeństwa i ulepszenia funkcjonalne. |
| Współpraca | Ze względu na funkcjonujące w urzędzie zabezpieczenia, oprogramowanie antywirusowe musi współpracować i być kompatybilne z obecnymi rozwiązaniami. |

1. UTM do klastra HA, licencja 2 lata

**Zakup urządzenia UTM do klastra HA wraz z licencją na 2 lata**

Zamawiający posiada rozwiązanie Sophos XGS 2100 i planuje dokupienie drugiego urządzenia, by sparować urządzenia i stworzyć klaster/redundantne rozwiązanie.

Zamawiający wymaga dostarczenia urządzenia Sophos XGS 2100.

Zamawiający wymaga również dostarczenia licencji do urządzenia Sophos XGS 2100 z subskrypcją 2 letnią licencji: Xstream Protection Data startu licencji 13.04.2025r.

1. Windows Server 2022 Std 4 szt + Windows Server 2022 Device CAL 100 szt.

Wymagana licencja na Windows Server 2022 Standard w ilości 4 szt., lub równoważne \*

Wymagana licencja na Windows Server 2022 Device CAL w ilości 100 szt., lub równoważne \*

Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory, które jest aktualnie wykorzystywane. Licencje zostaną wykorzystane do uruchomienia oprogramowana na nowych serwerach zakupionych w ramach niniejszego postępowania, jak również do modernizacji aktualnie posiadanych serwerów w urzędzie.

Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.

- Licencja bez ograniczeń czasowych. Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.

- instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;

- w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wieloprocesorowym;

- obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);

- wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;

- obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover)

– natywnie lub z wykorzystaniem sterowników producenta sprzętu;

- praca w roli klienta domeny Microsoft Active Directory;

- zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft WindowsServer 2022;

- zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);

- zawarta możliwość uruchomienia roli serwera DNS;

- zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);

- zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;

- zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;

- zawarta możliwość uruchomienia roli serwera stron WWW;

- zawarta funkcjonalność szyfrowania dysków;

- dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;

- w ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;

- w ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;

- 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).

\* 1. Ogólne warunki równoważności oprogramowania.

1.1) W przypadku zaoferowania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w OPZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że zaoferowane produkty spełniają wszystkie wymagania i warunki określone OPZ, w szczególności w zakresie:

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

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

1.c) 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,

1.d) poziomu zakłóceń pracy środowiska systemowo-programowego Zamawiającego spowodowanego wykorzystaniem zaoferowanych produktów równoważnych, który nie może być większy niż w przypadku produktów wymienionych w OPZ;

1.e) poziomu współpracy zaoferowanych produktów równoważnych z systemami Zamawiającego, który nie może być gorszy od tego jaki zapewniają produkty wymienione w OPZ,

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

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

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

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

1.j) dostępności wersji bitowych (32, 64) zaoferowanych produktów równoważnych, która nie może być mniejsza niż dla produktów wymienionych w OPZ;

1.k) dostępności wersji na różne systemy operacyjne zaoferowanych produktów równoważnych, która nie może być mniejsza niż dla produktów wymienionych w OPZ.

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

1.3) W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.

1.4) 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.

1.5) Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.

1.6) 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.

UWAGI DO OPZ:

1. Wymagania ogólne dotyczące przedmiotu zamówienia
	1. Wszystkie urządzenia muszą posiadać deklaracje CE;
	2. Opakowanie sprzętu musi gwarantować jego bezpieczny transport i składowanie;
	3. Zamawiający wymaga, by dostarczone urządzenia były fabrycznie nowe, wyprodukowane nie wcześniej niż na 6 miesięcy przed ich dostarczeniem. Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia. Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem.
	4. Na żądanie Zamawiającego Wykonawca, przed podpisaniem umowy, musi oświadczyć, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
	5. Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu. To wymagania dotyczy urządzeń, dla których producent przewiduje taką możliwość;
	6. Do każdego urządzenia musi być dostarczona dokumentacja w wersji elektronicznej w języku polskim. Jeżeli producent nie przewidział dokumentacji w języku polskim, Zamawiający dopuszcza dokumentację w języku angielskim. Zamawiający będzie miał prawo powielania dokumentacji na swój użytek w dowolnej liczbie kopii;
	7. W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z wymaganiami Zamawiający jest uprawniony do:
		1. zwrócenia się do producenta urządzeń o potwierdzenie ich zgodności z wymaganiami (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację),
		2. zlecenia producentowi oferowanych produktów lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych.
	8. Jeżeli inspekcja, o której mowa w pkt. 7 wykaże niezgodność oferowanych urządzeń z wymaganiami lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób trzecich, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 5% wartości zamówienia. Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z wymaganiami oraz roszczeń odszkodowawczych
	9. Wszystkie wymagane funkcjonalności muszą być dostępne w dniu składania oferty.
2. Dostawa
	1. Odbiorcami przedmiotu zamówienia jest Starostwo Powiatowe w Lęborku**,** 84-300 Lębork, ul. Czołgistów .
	2. Termin i godzina dostawy zostanie uzgodniona przez Wykonawcę, z co najmniej 3-dniowym wyprzedzeniem, z osobą uprawnioną do odbioru wskazaną w § 8 ust. 1 pkt 1 Umowy.
	3. Zamawiający stawia następujące warunki odnośnie harmonogramu dostaw :
		1. Wykonawca zobowiązany będzie do wniesienia urządzeń do pomieszczeń wskazanych przez odbiorcę;
		2. Zamawiający zastrzega sobie prawo sprawdzenia czy urządzenia są kompletne i nieuszkodzone;
		3. Przedstawiciel wykonawcy musi być obecny przy dostawie urządzeń i podpisywaniu protokołu

dostawy.

1. Warunki równoważności sprzętu:
	1. Oferowany sprzęt równoważny musi posiadać nie gorsze parametry techniczne, wydajnościowe oraz wszystkie wymagane funkcjonalności.
	2. Wszędzie tam, gdzie przedmiot zamówienia został opisany przez wskazanie nazwy, znaków towarowych lub pochodzenia a także norm, Zamawiający dopuszcza zaoferowanie przez Wykonawcę rozwiązania równoważnego.
	3. Wszystkie materiały, urządzenia, elementy wyposażenia przedstawione w przedmiotowej dokumentacji i opisane przez wskazanie znaków towarowych, patentów lub pochodzenia a także norm, należy traktować jako rozwiązania przykładowe o modelowych: parametrach technicznych i użytkowych, właściwościach charakterystycznych i właściwościach estetycznych, standardach określonych dla materiałów, urządzeń, elementów wyposażenia oraz warunków gwarancyjnych i serwisowych.
	4. Wszelkie nazwy własne znajdujące się w rekomendacjach – np. dotyczące urządzeń będących komponentami zestawu komputerowego, a także oprogramowania zostały przywołane jedynie przykładowo i nie mogą być w żaden sposób traktowane jako rekomendacja ich nabycia, użycia czy promocji.
	5. Powołanie przykładowej nazwy własnej nie może być interpretowane jako ocena właściwości danego urządzenia czy programu komputerowego, ani tym bardziej jako przesłanka uznania ich za lepsze od innych analogicznych urządzeń czy innego porównywalnego oprogramowania.
	6. Przez rozwiązanie równoważne dla wyspecyfikowanego przedmiotu zamówienia rozumie się takie, które w sposób poprawny współpracuje z infrastrukturą informatyczną Zamawiającego, a jego zastosowanie nie wymaga żadnych nakładów (finansowych, programistycznych, sprzętowych) związanych z dostosowaniem infrastruktury informatycznej Zamawiającego lub rozwiązania równoważnego oraz realizuje wszystkie funkcje i posiada wszystkie cechy określone w SWZ.
	7. Dopuszcza się zastosowanie rozwiązań równoważnych pod warunkiem zapewnienia wszystkich parametrów, właściwości i standardów oraz warunków gwarancyjnych i serwisowych nie gorszych niż określonych w opisie przedmiotu zamówienia oraz SWZ.
	8. W przypadku, gdy Wykonawca zaoferuje rozwiązanie równoważne, zobowiązany jest wykazać jego równoważność w stosunku do opisanego przedmiotu zamówienia.
	9. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy systemu informatycznego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem systemu informatycznego Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie systemu informatycznego Zamawiającego również po odinstalowaniu oprogramowania równoważnego.
	10. Oferowany sprzęt równoważny musi posiadać nie gorsze parametry techniczne, wydajnościowe oraz wszystkie wymagane funkcjonalności.
	11. Wszędzie tam, gdzie przedmiot zamówienia został opisany przez wskazanie nazwy, znaków towarowych lub pochodzenia a także norm, Zamawiający dopuszcza zaoferowanie przez Wykonawcę rozwiązania równoważnego.
	12. Wszystkie materiały, urządzenia, elementy wyposażenia przedstawione w przedmiotowej dokumentacji i opisane przez wskazanie znaków towarowych, patentów lub pochodzenia a także norm, należy traktować jako rozwiązania przykładowe o modelowych: parametrach technicznych i użytkowych, właściwościach charakterystycznych i właściwościach estetycznych, standardach określonych dla materiałów, urządzeń, elementów wyposażenia oraz warunków gwarancyjnych i serwisowych.
	13. Wszelkie nazwy własne znajdujące się w rekomendacjach – np. dotyczące urządzeń będących komponentami zestawu komputerowego, a także oprogramowania zostały przywołane jedynie przykładowo i nie mogą być w żaden sposób traktowane jako rekomendacja ich nabycia, użycia czy promocji.
	14. Powołanie przykładowej nazwy własnej nie może być interpretowane jako ocena właściwości danego urządzenia czy programu komputerowego, ani tym bardziej jako przesłanka uznania ich za lepsze od innych analogicznych urządzeń czy innego porównywalnego oprogramowania.
	15. Przez rozwiązanie równoważne dla wyspecyfikowanego przedmiotu zamówienia rozumie się takie, które w sposób poprawny współpracuje z infrastrukturą informatyczną Zamawiającego, a jego zastosowanie nie wymaga żadnych nakładów (finansowych, programistycznych, sprzętowych) związanych z dostosowaniem infrastruktury informatycznej Zamawiającego lub rozwiązania równoważnego oraz realizuje wszystkie funkcje i posiada wszystkie cechy określone w SWZ.
	16. Dopuszcza się zastosowanie rozwiązań równoważnych pod warunkiem zapewnienia wszystkich parametrów, właściwości i standardów oraz warunków gwarancyjnych i serwisowych nie gorszych niż określonych w opisie przedmiotu zamówienia oraz SWZ.
	17. W przypadku, gdy Wykonawca zaoferuje rozwiązanie równoważne, zobowiązany jest wykazać jego równoważność w stosunku do opisanego przedmiotu zamówienia.
	18. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy systemu informatycznego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem systemu informatycznego Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie systemu informatycznego Zamawiającego również po odinstalowaniu oprogramowania równoważnego.