**Załącznik nr 8 – Specyfikacja część II**

***Część II – Dostawa macierzy dyskowej, oprogramowania wraz z usługą wdrożenia wirtualizacji dla Powiatowego Urzędu Pracy w Stalowej Woli.***

**WYMAGANIA TECHNICZNE**

1. **Macierz dyskowa.**

Ilość – 1 szt.

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagane minimalne** |
| Obudowa: | O wysokości maksymalnie 2U, do instalacji w standardowej szafie RACK 19” dostarczona wraz ze wszystkimi elementami umożliwiającymi instalację.  Możliwość instalacji minimum 12 dysków twardych Hot-Plug 2,5”. |
| Możliwość rozbudowy: | Bez wymiany kontrolerów macierzy o dodatkowe co najmniej 72 dysków twardych 2,5”, lub dodatkowe co najmniej 36 dysków twardych 3,5”. |
| Kontrolery: | Minimum 2 kontrolery RAID pracujące w układzie active-active  Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników.  Wraz z macierzą należy dostarczyć minimum 4 kable SAS 12Gb HD-Mini SAS o długości min. 2 metry. |
| Interfejsy kontrolera: | Minimum:  - 1 port 1GbE RJ-45 LAN (zarządzanie),  - 2 porty 12Gb SAS 12Gb/s (do podłączania serwerów). |
| RAID: | Obsługa RAID zgodne z minimum RAID1, RAID10, RAID3, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych.  Możliwość definiowania dysków hot-spare. |
| Cache: | Minimum 8GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inną pamięć nieulotną zabezpieczoną za pomocą podtrzymania bateryjnego w razie awarii zasilania. |
| Obsługa dysków: | SSD, SAS i Nearline SAS. Możliwość mieszanie napędów dyskowych w obrębie pojedynczej półki dyskowej i macierzy. Obsługa dysków 2,5”  oraz 3,5”. |
| Dostarczone dyski twarde: | 12 dysków twardych SSD Hot–Swap z interfejsem SAS 12GB/s lub SAS 24 Gb/s o pojemności minimum 1.92TB o parametrze 1DWD zgodne z listą kompatybilności oferowanej macierzy. |
| Zarządzanie macierzą: | Z poziomu interfejsu graficznego i interfejsu znakowego, bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi  oraz dyskami logicznymi: | Możliwość zdefiniowanie, minimum 500 wolumenów logicznych.  Możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Udostępnianie zasobów: | Możliwość udostępniania zasobów dyskowych do serwerów w trybie tradycyjnym oraz w trybie typu Thin Provisioning.  Możliwość odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Zdalna replikacja danych: | Możliwość co najmniej asynchronicznej replikacji danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.  Możliwość aktywowania tej funkcjonalności w przyszłości dla całej pojemności macierzy. |
| Wsparcie dla systemów operacyjnych: | Możliwość jednoczesnego podłączenia wielu serwerów w trybie wysokiej dostępności minimum dwoma ścieżkami.  Wsparcie dla: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware vSphere.  Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów – Dołączyć wydruk do oferty. |
| Bezpieczeństwo: | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. |
| Dodatkowe wymagania: | Oferowany sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.  Elementy, z których zbudowana jest macierz muszą być produktami producenta macierzy, lub być przez niego certyfikowane, oraz muszą być objęte gwarancją producenta. Na żądanie Zamawiającego, Wykonawca dostarczy wraz ze sprzętem oświadczenia producenta potwierdzające, że oferowany sprzęt spełnia te wymogi.  Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.  Urządzenie musi być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.  Oferowany system dyskowy musi składać się z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Macierz musi umożliwiać szyfrowanie z wykorzystaniem dysków SED.  Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| Gwarancja: | Producenta, minimum 36 miesięcy na urządzenie i minimum 36 miesięcy na dyski gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji maksymalnie do następnego dnia roboczego od przyjęcia zgłoszenia.  W przypadku awarii dysku twardego dysk pozostaje u Zamawiającego. |
| Wsparcie techniczne: | Możliwość pobierania uaktualnień, poprawek i sterowników. |
| Dokumentacja użytkownika: | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |

1. **Oprogramowanie – backup i archiwizacja danych.**

|  |
| --- |
| **Wymagane minimalne** |
| Licencja wieczysta z rocznym wsparciem producenta. Ilość licencji musi umożliwiać robienie kopii wszystkich maszyn wirtualnych używanych przez Zamawiającego, tj. 9 szt. oraz musi być zgodna z ilością serwerów w klastrze wirtualizacyjnym. **Wymagania ogólne:**  * Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. * Oprogramowanie musi współpracować z posiadaną przez Zamawiającego infrastrukturą Vmware Essentials 8 Plus Kit. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej; * Oprogramowanie musi współpracować z posiadanymi przez Zamawiającego hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami; * Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich posiadanych przez Zamawiającego systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere. * Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.  **Całkowite koszty posiadania:**  * 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 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 tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. * Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. * Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania. * Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time). * 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 posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. * Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej. * Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora). * Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS). * Oprogramowanie musi posiadać integracje z systemami typu SIEM. * Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.  **Wymagania RPO:**  * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. * Oprogramowanie musi wykorzystywać mechanizmy 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 z dokładnością do pojedynczego datastoru. * 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.. * Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. * Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). * Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). * Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. * 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. * 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 możliwość 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).  **Wymagania RTO:**  * 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 pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. * 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/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. * Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell. * Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM. * 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, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1  i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku  point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013  i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. * 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 wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych  w środowiskach Linux. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji. * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN. * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle. * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI. * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2. * Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.  **Ograniczenie ryzyka:**  * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). * Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz 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 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 analizować indeksy systemów plików zabezpieczanych maszyn  w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware. * Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania. * Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi  w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków. * Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.   **Środowisko fizyczne:**   * Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. * Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych. * Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE. * Rozwiązanie musi wspierać system operacyjny macOS. * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix. * Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą). * Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster. * Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. * Rozwiązanie musi wspierać backup podłączonych dysków USB. * Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. * Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury). * Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. * Rozwiązanie musi wspierać kontrolę pasma sieciowego. * Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. * Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. * Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. * Rozwiązanie musi wspierać technologię BitLocker. * Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. * Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych. * Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. * Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. * Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. * Rozwiązanie musi wspierać szyfrowanie. * Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne. * Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego. * Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej. * Rozwiązanie musi wspierać tworzenie wielu zadań backupowych  **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 6.x, 7.x oraz 8.0 – 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 2012, 2012R2, 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 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. * System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4.  **Raportowanie:**  * System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. * System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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 wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. * System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V. * System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF. * System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc. * System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach. * System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów. * System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych. * System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych. * System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz  z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury. * System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta. * System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. * System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. * System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware. * System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots). * System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie. |

1. **Oprogramowanie systemowe.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Wyszczególnienie** | **Ilość (szt.)** |
| 1. | Windows Server 2022 Standard (16 core) lub nowszy | 2 |
| 2. | Windows Server 2022 Standard CAL lub nowszy | 70 |

1. **Wdrożenie**

Ilość – 1 szt.

Celem prac montażowo konfiguracyjnych jest odtworzenie jeden do jednego istniejącego środowiska wirtualnego oraz istniejącej infrastruktury serwerowni Zamawiającego w oparciu o nowo zakupiony sprzęt.

Zamawiający dopuszcza wykonanie wizji lokalnej w serwerowni oraz w środowisku informatycznym Zamawiającego przed przystąpieniem do prac wdrożeniowych.

**Zamawiający do wykonania niżej opisanych zadań oprócz dostarczonego w niniejszym postępowaniu sprzętu zakłada wykorzystanie posiadanych przez Zamawiającego 2 nowych serwerów: FUJITSU PRIMERGY RX2540 M6.**   
Procesor: 2x 2,8GHz 8-rdzeni.   
RAM: 128 GB DDR4 320 MHz.   
SSD: 2 x 240GB M.2.   
Kontroler SAS: Fujitsu PSAS CP500e FH/LP

Prace te obejmują m.in.:

1. Demontaż starych serwerów – 3 szt.
2. Fizyczny montaż nowych serwerów w szafie serwerowej – 2 szt.
3. Fizyczny montaż nowej macierzy w szafie serwerowej – 1 szt.
4. Podłączenie zasilania do nowych serwerów (wymagana redundancja połączenia) – 2 szt.
5. Podłączenie zasilania do nowej macierzy (wymagana redundancja połączenia) – 1 szt.
6. Podłączenie do sieci LAN każdego serwera do 3 wykorzystywanych switch’y (redundancja połączenia).
7. Podłączenie do sieci LAN macierzy (redundancja połączenia).
8. Podłączenie portów zdalnego sterowania serwerem do switchy.
9. Wykonanie procedury aktualizacji firmware dostarczonych serwerów oraz macierzy do najnowszej wersji oferowanej przez producenta danego sprzętu.
10. Kompleksowe przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego.
11. Kompleksowe przygotowanie dostarczonej macierzy dyskowej pod kontem gotowości do pracy (wolumeny, pule, miejsce na przechowywanie).
12. Instalacja VMWare na nowych serwerach – 2 szt.
13. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta (na dostarczone konto Urzędu).
14. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.
15. Uruchomienie klastra wysokiej dostępności w oparciu o nowe serwery i nową macierz.
16. Konfiguracja mechanizmów HA - w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
17. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
18. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
19. Weryfikacja działania klastra wysokiej dostępności.
20. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
21. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego macierzy. Wymaga się takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
22. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN.
23. Migracja i uruchomienie istniejących maszyn wirtualnych.
24. Instalacja nowego lub aktualizacja istniejącego oprogramowania do zarządzania środowiskiem wirtualizacyjnym.
25. Aktualizacja systemu Ms Windows Serwer 2012 używanego, jako kontroler Domeny do Windows Serwer 2022.
26. Weryfikacja działania po aktualizacji wszystkich serwerów i usług niezbędnych do prawidłowego funkcjonowania środowiska serwerowego Zamawiającego. Wymagana inwentaryzacja serwerów i usług przed przystąpieniem do aktualizacji.
27. Aktualizacja systemu Ms Windows Serwer 2012 używanego, jako serwer baz danych do Windows Serwer 2022, oraz uruchomienie na nim zapasowego kontrolera Domeny.
28. Weryfikacja działania po aktualizacji wszystkich serwerów i usług niezbędnych do prawidłowego funkcjonowania środowiska serwerowego Zamawiającego. Wymagana inwentaryzacja serwerów i usług przed przystąpieniem do aktualizacji.
29. Instalacja systemu Ms Windows Serwer 2022 na nowych maszynach wirtualnych – 2 szt.
30. Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych na nowo zainstalowanym serwerze Windows Serwer 2022.
31. Kompleksowe przygotowanie istniejącej macierzy wykorzystywanej wcześniej (DELL MD3420) , jako macierz produkcyjna do pracy z serwerem backupu.
32. Podłączenie przestrzeni dyskowej przygotowanej wcześniej macierzy, do serwera backupu.
33. Podłączenie przestrzeni dyskowej istniejącego serwera NAS do serwera backupu. Istniejące kopie zapasowe obrazów maszyn wirtualnych muszą pozostać na serwerze NAS.
34. Aktywacja wymaganych licencji.
35. Wykorzystanie i wdrożenie koncepcji backupu w oparciu o schemat DISK-to-DISK (macierz produkcyjna – macierz backupu).
36. Konfiguracja zadań wykonywania kopii zapasowych wirtualnych maszyn według poniższych wymagań:
37. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
38. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
39. kopie maszyn wirtualnych muszą być replikowane na wskazany przez Zamawiającego zasób dyskowy
40. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
41. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
42. musi istnieć możliwość odtworzenia:

* całej wirtualnej maszyny;
* dysku wirtualnej maszyny;
* pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa);
* konfiguracja powiadomień o wykonaniu kopii zapasowej (e-mail).

1. Zduplikowanie istniejących kopii obrazów maszyn wirtualnych z serwera NAS na przygotowaną wcześniej macierz.
2. Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia, w ramach jednego weekendu (piątek godz. 16:00 – Niedziela godz. 22:00)**\*** po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym. Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszych dwóch dni roboczych następujących po pracach wdrożeniowo – instalacyjnych w godzinach od 7.30 do 16.00. W tym czasie przedstawiciele Wykonawcy zobowiązani są do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. W tym czasie przedstawiciele Wykonawcy dokonają także przeszkolenia pracownika Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań.

**\*** *Zamawiający dopuszcza, aby wszystkie prace nie kolidujące z pracą Urzędu (np. aktualizacja serwerów, instalacja środowiska wirtualizacyjnego, itp.) mogły być wykonywane w ciągu dnia roboczego w godzinach pracy Urzędu. Zakres tych prac Zamawiający ustali z Wykonawcą.*

1. Zamawiający wymaga świadczenia opieki serwisowej w ilości 10 godzin miesięcznie, przez okres minimum 6 miesięcy, od momentu podpisania protokołu odbioru, z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny, z zakresu realizowanego wdrożenia oraz powstałego sytemu teleinformatycznego. Czas reakcji jest rozumiany, jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych. Niewykorzystana pula godzin w danym miesiącu przechodzi na kolejny miesiąc sumując się.
2. Wykonawca zapewni przyjmowanie zgłoszeń w godzinach roboczych, przez które rozumie się godziny od 8:00 do 15:00 w dni robocze.
3. Prace serwisowe mogą być również realizowane po godzinach pracy Urzędu w tym również w dni wolne. Termin realizacji prac Zamawiający uzgadnia z Wykonawcą. Priorytetem jest jednak jak najszybsze usunięcie awarii i przywrócenie pracy środowiska informatycznego Zamawiającego.
4. Prace serwisowe niewymagające fizycznej obecności serwisanta w siedzibie Zamawiającego, mogą być wykonywane zdalnie.
5. W przypadku, jeżeli producent standardowego oprogramowania systemowego, standardowego oprogramowania aplikacyjnego lub sprzętu komputerowego udostępni jakiekolwiek aktualizacje, nowe wersje, patche, zmiany itp. (dalej łącznie zwane aktualizacjami), Wykonawca w ramach usług serwisu zapewni Zamawiającemu wykonanie takich aktualizacji, nie rzadziej niż co 2 miesiące, a jeżeli będą to aktualizacje krytyczne bezpieczeństwa niezwłocznie powiadomi Zamawiającego o ich dostępności i ustali termin wdrożenia.
6. W przypadku stwierdzenia, że przyczyna wady leży w standardowym oprogramowaniu systemowym, standardowym oprogramowaniu aplikacyjnym lub oprogramowaniu dostarczanym przez Wykonawcę w ramach infrastruktury technicznej, Wykonawca w czasie naprawy jest zobowiązany do wykonania obejścia, a do usunięcia wady jest zobowiązany niezwłocznie po zapewnieniu odpowiedniej poprawki przez producenta standardowego oprogramowania systemowego lub standardowego oprogramowania aplikacyjnego. W celu uniknięcia wątpliwości w takim przypadku wykonanie obejścia w czasie naprawy stanowi należyte wykonanie umowy i nie jest podstawą do naliczenia kar umownych z tytułu niedochowania czasu naprawy, co nie zwalnia Wykonawcy z obowiązku usunięcia wady po udostępnieniu odpowiedniej poprawki przez producenta oprogramowania.
7. Wykonawca przygotuje i przekaże Zamawiającemu dokumentację powykonawczą obejmującą konfigurację dostarczonego sprzętu, a w szczególności:

* Opis przeprowadzonych prac;
* Zestawienie danych inwentarzowych;
* Opis konfiguracji macierzy dyskowej;
* Opis konfiguracji klastra HA;
* Opis konfiguracji systemu kopii zapasowej.