Załącznik nr 1
do Informacji o ogłoszeniu z dnia 09.11.2022r.

OPIS PRZEDMIOTU ZAMÓWIENIA

WYMAGANE PARAMETRY TECHNICZNE

1. Serwer kopi zapasowej i kopi bezpieczeństwa

Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Możliwość zainstalowania minimum 16 dysków twardych hot plug; • Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych; • Zainstalowane minimum 6 szt. dysków SSD SATA minimum 960GB, DWPD min 3; • Możliwość zainstalowania dedykowanego wewnętrznego napędu CD/DVD.

Płyta główna	• Dwuprocesorowa;
	• Możliwość instalacji procesorów 38-rdzeniowych;
	• Możliwość zainstalowania modułu TPM 2.0;
	• Złącza PCI Express nie gorsze niż 4 generacji
	• Gniazda pamięci RAM;
	• Obsługa minimum 4TB pamięci RAM;
	• Wsparcie dla technologii:
	  ○ Advanced ECC,
	  ○ Memory Page Retire,
	  ○ Fault Resileint Memory,
	  ○ Memory Self-Healing,
	  ○ Partial Cache Line Sparing
	  ○ Memory Health Check,
	  ○ Memory Page Retire
	• Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)

Procesory	• Minimalnie dwa procesory 12-rdzeniowy • Taktowanie nie może być wolniejsze niż 2,6 GHz • architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 212 pkt (wynik osiągnięty dla zainstalowanych dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html
Pamięć RAM	• nie mniej niż 256 GB pamięci RAM • DDR z rejestrem pozwalającym na zwiększenie stabilności systemy podczas wykorzystywania większej ilości modułów pamięci. • nie wolniejsze niż 3200MHz
Kontrolery LAN	• Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 10Gbit Base-T, • Dodatkowa karta zainstalowana w slocie PCIe 2x 10Gbit SFP+, wszystkie porty obsadzone modułami MMF LC • Wbudowane dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 • Dla każdego portu SFP28 należy dostarczyć kabel direct attach SFP28 do SFP28 o długości min. 3 metry
Kontrolery I/O	• Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde • Zainstalowany wewnętrzy kontroler SAS RAID obsługujący poziomy 0,1,5,6,10,50,60 obsługujący zaoferowane dyski twarde;
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; • Minimum 1 porty USB 2.0; • Przynajmniej 1 porty USB-3.0 na panelu przednim • Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;

	• Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 94% o mocy minimalnej 800W; • Redundantne wentylatory hotplug;
Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii • 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 • TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • 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 ośmiu 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 umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • 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
Wspierane OS	• Microsoft Windows Server 2022, 2019, 2016 • VMWare vSphere 6.7, 7.0 • Suse Linux Enterprise Server 15 • Red Hat Enterprise Linux 7.9, 8.3
Gwarancja	• 24 miesięcy gwarancji w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub serwis autoryzowany przez producenta. • Funkcja zgłaszania usterek i awarii sprzętowych w systemie helpdesk/servicedesk producenta sprzętu lub autoryzowanego przedstawiciela producenta; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • 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

Dokumentacja, inne	• Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem np. strony www producenta serwera lub autoryzowanego przedstawiciela; • Zgodność z normami: CB, RoHS, WEEE, GS oraz CE;

Wymagania ogólne wobec urządzeń, opisanych powyżej:

1. Zamawiający wymaga, by dostarczony sprzęt był nowy oraz nieużywany (przy czym Zamawiający dopuszcza, by sprzęt był rozpakowany i uruchomiony przed jego dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania sprzętu, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem),
2. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Zamawiającemu nie mogą być zaoferowane sprzęt i oprogramowanie, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
3. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej w dniu poprzedzającym dzień składania ofert,
4. Wymagane jest, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania.
5. Zaoferowane urządzenia nie mogą być na dzień składania ofert przeznaczone przez producenta do wycofania z produkcji.
6. Wymagane jest, aby data produkcji dostarczonych urządzeń nie była wcześniejsza niż 12 miesięcy od daty ogłoszenia postępowania.

2. System serwerowy

Zamawiający wymaga dostarczenie w ramach postępowania następujących licencji oprogramowania.
1. Microsoft Windows Server 2022 standard licencja dla dwóch procesorów 12 rdzeniowyc lub równoważna.
Dostarczone licencje muszą sumarycznie pozwalać na nielimitowane używanie oprogramowania Microsoft Windows Server 2022 (i wersji wcześniejszych).
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy równoważności:

1. Możliwość wykorzystania (w ramach ilości posiadanych licencji) nielimitowanej liczby rdzeni logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.

7. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   7.1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   7.2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   7.3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   7.4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.
13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   14.1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   14.2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17. Mechanizmy logowania w oparciu o:
   17.1. Login i hasło,
   17.2. Karty z certyfikatami (smartcard),
   17.3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
18. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci,
19. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   25.1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   25.2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
   25.3. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
   25.4. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
   25.5. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
   25.6. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
   25.7. Zdalna dystrybucja oprogramowania na stacje robocze.
   25.8. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
   25.9. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
26. Dystrybucję certyfikatów poprzez http
27. ii. Konsolidację CA dla wielu lasów domeny,

28. iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    28.1. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    28.2. Szyfrowanie plików i folderów.
    28.3. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    28.4. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
    28.5. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    28.6. Serwis udostępniania stron WWW.
    28.7. Wsparcie dla protokołu IP w wersji 6 (IPv6),
    28.8. Wsparcie dla algorytmów Suite B (RFC 4869),
    28.9. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    28.10. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
    28.11. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
    28.12. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
    28.13. Mechanizmy wirtualizacji mające wsparcie dla:
        28.13.1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
        28.13.2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
        28.13.3. Obsługi 4-KB sektorów dysków
        28.13.4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    28.14. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    28.15. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
    28.16. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
29. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
30. Wsparcie dla rozwiązania Kubernetes.
31. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
32. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
33. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
34. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
35. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
36. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
37. Mechanizm konfiguracji połączenia VPN do platformy Azure.
38. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
39. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
40. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

3. System do wirtualizacji

Wymagane jest dostarczenie 2 szt. licencji oprogramowania do tworzenia serwerów wirtualnych spełniającego poniższe wymagania minimalne:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

3. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
9. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
10. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
11. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
15. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
16. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
17. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
18. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania lub autoryzowanego partnera. Licencjonowanie nie może odbywać się w trybie OEM.
19. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
20. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
21. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
22. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
23. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
24. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
25. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,

26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
27. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
28. Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej.
29. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
    Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.
30. Oprogramowanie musi posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych
31. Oprogramowanie musi umożliwiać globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych
32. Oprogramowanie musi umożliwiać wykonywanie automatycznych bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych.
33. Rozwiązanie musi zapewniać widok całego systemu i zbioru maszyn wirtualnych - Mapy Infrastruktury.
34. Rozwiązanie musi umożliwiać monitorowanie dostępności i wydajności maszyn wirtualnych
35. Oprogramowanie musi mieć możliwość raportowania dostępności i wydajności maszyn wirtualnych
36. Rozwiązanie musi posiadać funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows
37. Musi umożliwiać planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych
38. Oprogramowanie musi umożliwiać tworzenie obrazów maszyn wirtualnych oraz klonowanie maszyn wirtualnych
39. Rozwiązanie musi umożliwiać wykonywanie wielu kopii migawkowych (snapshoot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii

4. System do backupu danych

Wymagane jest dostarczenie 1 kompletu licencji oprogramowania do tworzenia kopi zapasowych oraz bezpieczeństwa dla środowiska działającego u Zamawiającego. Licencje muszą być dożywotnie i uwzględniać wsparcie na minimum 36 miesięcy. System kopii musi obejmować następujące elementy:

1. 20 serwerów wirtualnych uruchomionych w środowisku Hyper-V.
2. 10 serwerów fizycznych
3. Klaster dwóch serwerów bazodanowych Oracle, zbudowany w środowisku Linux
4. Nowe środowisko wirtualne serwerów bazodanowych Oracle Standard Edition, zbudowane na VMware vSphere 7 Standard z vCenter Server 7 Standard
5. Klaster serwerów plików dostępnych dla użytkowników usług katalogowych
6. Serwer poczty elektronicznej uruchomiony w systemie Linux

Oprogramowanie musi spełniać poniższe wymagania minimalne:

1. 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.
2. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowe

3. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
4. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
5. 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
6. 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.
7. 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.
8. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, 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.
9. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
10. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
11. 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)
12. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
13. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
14. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
15. 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
16. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
17. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
18. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
19. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
20. Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
21. 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
22. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
23. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
24. 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, Huawei, INFINIDAT, Pure Storage.
25. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
26. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
27. Oprogramowanie musi posiadać wsparcie dla NDMP

28. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
29. 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.
30. 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.
31. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 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)
32. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
33. 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.
34. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwosc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
35. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
36. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
37. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
38. 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 oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
39. 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
40. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
41. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
42. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
43. 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
44. 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.
45. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
    a. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
    b. BSD: UFS, UFS2
    c. Solaris: ZFS, UFS
    d. Mac: HFS, HFS+
    e. Windows: NTFS, FAT, FAT32, ReFS
    f. Novell OES: NSS
46. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
47. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
48. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
49. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.

50. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
51. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
52. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
53. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
54. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
55. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
56. 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.
57. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
58. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
59. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
60. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
61. 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.
62. 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
63. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
64. 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, Comodo.
65. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
66. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
67. 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
68. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
69. System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware
70. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
71. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
72. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
73. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
74. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
75. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
76. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
77. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
78. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

79. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
80. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
81. 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.
82. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
83. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x
84. Raportowanie
85. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2019 oraz 2022
86. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
87. System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
88. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
89. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
90. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
91. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
92. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
93. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
94. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
95. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
96. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
97. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
98. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
99. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
100. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
101. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

5. Wdrożenie

Celem wdrożenia jest:

1. stworzenie i przetestowanie systemu do tworzenie kopi zapasowych,

Niezbędne jest również utworzenie procedur użytkowych i zapewniających ciągłość pracy systemu tworzenia kopii zapasowych i disaster recovery w oparciu o dostarczone w niniejszym postepowaniu urządzenia i oprogramowanie.

Instalacje i konfiguracje elementów systemu mają odbywać się zgodnie z najlepszymi praktykami przedstawianymi przez producentów poszczególnych urządzeń i oprogramowania.

Wszystkie prace wdrożeniowe muszą zostać wykonane w obecności pracownika Zespołu ds. Informatyki bez przerywania pracy systemów, w dniach i godzinach roboczych. Dopuszcza się możliwość wykonywania części prac zdalnie poprzez bezpieczne połączenie SSL-VPN na zasadach określonych przez Zespół ds. Informatyki na wniosek Wykonawcy.

W szczególnych przypadkach gdy wymagane będzie wstrzymanie pracy systemów Szpitala działania takie muszą zostać skonsultowane i zaakceptowane przez Zespół ds. Informatyki, z co najmniej trzy dniowym wyprzedzeniem
Dostarczane do Zamawiającego w ramach przedmiotu umowy, urządzenia należy wyposażyć we wszystkie niezbędne interfejsy i okablowanie tak, aby możliwe było zrealizowanie opisanych w SWZ funkcjonalności. Do urządzeń muszą być dostarczone wszystkie wymagane licencje umożliwiające poprawną prace urządzeń w zakresie wymaganych w SWZ funkcjonalności.

Zamawiający wymaga instalacji dostarczanych rozwiązań przez wykwalifikowany personel.

W ramach realizacji przedmiotu zamówienia Wykonawca będzie zobowiązany do:

1. przygotowania planu i harmonogramu wdrożenia,
2. dostawy, montażu i instalacji poszczególnych komponentów systemu,
3. konfiguracji urządzeń i oprogramowania zgodnie z planem wdrożenia,
4. wykonania testów działania urządzeń i oprogramowania oraz całości rozwiązania,
5. opracowanie i wdrożenie procedur użytkowych,
6. opracowanie i wdrożenie procedur odzyskania pełnej sprawności systemu po awarii,
7. wykonania dokumentacji powykonawczej,
8. przeprowadzenia bezpłatnego instruktażu dla administratorów Zamawiającego,

Wszystkie prace muszą być prowadzone z zachowaniem należytej staranności, zgodnie z najlepszymi praktykami branżowymi.

Wykonawca opracuje plan wdrożenia w ciągu 3 dni roboczych od dnia podpisania Umowy.
Plan wdrożenia będzie wykonany przez Wykonawcę w oparciu o najlepsze praktyki branżowe, zgodnie z wytycznymi producentów oferowanych rozwiązań. W ramach Planu wdrożenia Wykonawca przygotuje następujące dokumenty:

1. Szczegółowy Plan Wdrożenia,
2. Harmonogram Wdrożenia.

Plan oraz Harmonogram wdrożenia zostaną zaakceptowane przez Zamawiającego w terminie najpóźniej 5 dni roboczych od daty jego złożenia. W razie wystąpienia uwag Zamawiającego do powyższych dokumentów, Wykonawca jest zobowiązany nanieść poprawki w terminie 2 dni roboczych, a Zamawiający zaakceptuje poprawki również maksymalnie w ciągu 2 dni roboczych.
Szczegółowy Plan Wdrożenia obejmować będzie określenie szczegółowo wszystkich parametrów logicznych i fizycznych dla urządzeń, oprogramowania i usług objętych przedmiotem zamówienia, w tym w szczególności: plan montażu i podłączenia sprzętu, podłączenie zasilania, konfiguracje sieci LAN (adresacje IP sieci zarządzania i produkcyjne, wdrożenie i podział VLANów), podłączenie i konfigurację sieci SAN, konfigurację urządzeń i oprogramowania, nazewnictwo, plan testów odbiorczych.
Harmonogram obejmował będzie:

1. termin rozpoczęcia realizacji prac liczony od momentu podpisania umowy,
2. termin zakończenia realizacji prac,
3. podział prac na etapy, termin i czas trwania poszczególnych etapów, zależności pomiędzy poszczególnymi etapami,
4. osoby odpowiedzialne ze strony Wykonawcy za realizacje poszczególnych etapów,
5. termin odbioru,
6. harmonogram winien być sporządzony w postaci pliku MS Excel lub równoważnego.

Kwalifikacje muszą być potwierdzone certyfikatami wystawianymi przez producenta oferowanego rozwiązania w zakresie instalacji oraz wdrożenia dostarczanych rozwiązań. Certyfikaty należy przedstawić na każde żądanie Zamawiającego po podpisaniu umowy.

1. Serwer oraz oprogramowanie należy dostarczyć do siedziby Zamawiającego, rozładować i wnieść do wskazanego przez Zamawiającego miejsca. Zainstalować w szafach RACK Zamawiającego i podpiąć do istniejącej infrastruktury zgodnie z ustaleniami poczynionymi z Zamawiającym.
2. Wykonawca w ramach wdrożenia dostarczy, zamontuje, zainstaluje, skonfiguruje i dostosuje do potrzeb Zamawiającego całość sprzętu i oprogramowania będącego przedmiotem umowy. W zakresie takim, aby możliwe było ich użytkowanie przez Zamawiającego zgodnie z przeznaczeniem i celem zakupu.
3. Zamawiający wymaga by zarówno macierz uruchomiona i działająca u Zamawiającego jak również dostarczone serwery były połączone za pomocą sieci SAN.
4. Zamawiający wymaga konfiguracji dostarczonego serwera zgodnie z wymaganiami Zamawiającego.
5. Zamawiający wymaga uruchomienia dostarczonego serwera zgodnie z wymaganiami licencyjnymi zakupionego oprogramowania.

6. Zamawiający wymaga stworzenie systemu do tworzenia kopii zapasowych dla wszystkich kluczowych danych w systemach Zamawiającego.

Wymagania dodatkowe

Zamawiający wymaga przeprowadzenia szkoleń personelu Zespołu ds. Informatyki na poziomie eksperta z zakresy wdrożonych systemów obsługi poczty elektronicznej, tworzenia kopi zapasowych oraz systemu do monitorowania zdarzeń niepożądanych. Szkolenia obejmują 4 osoby.

1. W ramach udzielonej gwarancji - przez okres 24 miesięcy od daty podpisania Końcowego Protokołu Odbioru – bezusterkowego, Wykonawca zapewni pełną funkcjonalność systemu w skład którego wchodzą dostarczone urządzenia i oprogramowanie - poprzez bezpłatne usuwanie awarii, usterek i wad dostarczonych urządzeń, dostarczanie nowych wersji oprogramowania oraz udzielanie bezpłatnych konsultacji.
2. Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, tj. by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta.
3. Zamawiający zastrzega, że serwis usług gwarancyjnych ma być świadczony w miejscu instalacji urządzeń.
4. Wymagane godziny pracy serwisu Wykonawcy: 7.30-15.30 od poniedziałku do piątku w dni robocze.
5. Wymagany czas reakcji serwisu Wykonawcy na zgłoszenie serwisowe: max. 4 godziny od momentu zaewidencjonowania zgłoszenia serwisowego przez Użytkownika Zamawiającego. Zamawiający wymaga by w czasie max. 4 godzin, o których mowa w zdaniu poprzednim, Wykonawca nadał zgłoszeniu serwisowemu status warunkujący jego realizację lub odrzucenie.
6. Użytkownik Zamawiającego będzie miał możliwość zaewidencjonować następujące zgłoszenia serwisowe:
   6.1. awaria - oznacza sytuację, w której nie jest możliwe prawidłowe używanie części lub całości uruchomionego systemu.
   6.2. usterka - błąd, mimo identyfikacji którego nadal funkcjonuje system lecz jego eksploatacja jest uciążliwa, skomplikowana lub spowolniona, a usuniecie błędu wymaga wykonania prac serwisowych inżynierów danej specjalności.
   6.3. konsultacja - usługa świadczona przez Wykonawcę polegająca na bieżącym udzielaniu Zamawiającemu wyjaśnień w kwestiach dotyczących działania systemu w całości lub jego części.
7. Obsługa zgłoszenia serwisowego przebiegać powinna na zasadach określonych we wskazanych niżej procedurach realizacji przewidzianych dla poszczególnych usług:
7.1. Awaria
7.2. Usterka
7.3. Konsultacje

Zasady świadczenia usług – tabela skrócona:

L.p.	Rodzaj świadczonych usług	Czas wykonania zlecenia serwisowego	Warunki świadczenia usług
2.	Usterka	czas usunięcia – max. 5 dni roboczych lub najbliższa aktualizacja systemu.	O przedłużeniu czasu usunięcia usterki Wykonawca poinformuje z 2 dniowym wyprzedzeniem czyli naj później 1 dzień przed końcem maksymalnego czasu realizacji usunięcia usterki.
3.	Awaria	czas usunięcia – 36 h	Czas liczony w godzinach od upływu czasu reakcji serwisu Wykonawcy do momentu usunięcia awarii.
3.	Konsultacja	czas wykonania max. 10 dni roboczych	Czas liczony w dniach roboczych od upływu czasu reakcji serwisu Wykonawcy. Zamawiający przewiduje 10 godzin na każde 12 miesięcy gwarancyjnych usług serwisowych.

Szczegółowy zakres oraz warunki realizacji usług:
1. Usterka
1.1. Zgłoszenie serwisowe będzie wysyłane do Wykonawcy od poniedziałku do piątku w dni robocze, w godzinach od 7:30 do 15:30.
1.2. Czas usunięcia błędu: max do 5 dni roboczych liczonych od upływu czasu reakcji serwisu Wykonawcy na zgłoszenie serwisowe do dnia usunięcia błędu.

1.3. Po usunięciu błędu i wykonaniu testu poprawnego działania systemu, zaakceptowanego przez Zamawiającego, zgłoszenie serwisowe traktowane jest jako zakończone. Testy wykonywane są w dniu zgłoszenia przez Wykonawcę usunięcia usterki lub w dniu roboczym następnym.

2. Awaria

2.1. Czas usunięcia awarii - maksymalnie 36 godzin od upływu czasu reakcji serwisu Wykonawcy do godziny całkowitego usunięcia awarii i wykonania przez Wykonawcę testu poprawnego działania systemu, zaakceptowanego przez Zamawiającego.

2.2. Po usunięciu awarii i wykonaniu przez Wykonawcę testu poprawnego działania systemu, zaakceptowanego przez Zamawiającego, zgłoszenie serwisowe traktowane jest jako zakończone.

2.3. Zgłoszenie serwisowe jest ostatecznie zamykane jeżeli upłynęło 14 dni od terminu usunięcia Awarii i wykonania testu systemu zaakceptowanego przez Zamawiającego, a Zamawiający nie wniósł w tym czasie zastrzeżeń do wyniku.

3. Konsultacja

3.1. Przyjęcie zgłoszenia Konsultacji związane jest z podjęciem następujących działań:

3.1.1. wskazanie Użytkownikowi w dokumentacji lub materiałach szkoleniowych zapisów, w których znajdują się informacje dotyczące przedmiotu zgłoszenia serwisowego,

3.1.2. wskazanie Użytkownikowi miejsca, w którym można powziąć informacje na temat przedmiotu zgłoszenia, jeżeli było ono uprzednio przedmiotem działań serwisowych inicjowanych przez innych Użytkowników, w szczególności do zamieszczonych w serwisie.

3.1.3. udzielenie konsultacji i wyjaśnień w kwestiach stanowiących przedmiot zgłoszenia.

3.2. Po uznaniu przez Użytkownika i pracownika serwisu, że jego realizacja dobiegła końca, status zgłoszenia zmienia się na zakończone.

Po upływie 14 dni od terminu, w którym zgłoszenie serwisowe uzyskało status zakończone, a Użytkownik nie wniósł do niego zastrzeżeń, zgłoszenie serwisowe jest ostatecznie zamykane.

Opracował Rafał Skorus