# **Opis przedmiotu zamówienia, wymagane parametry techniczne oraz wymagania dotyczące wdrożenia**

**Po zmianie z dnia 04.07.2023r.**

### **Pakiet 1**

**System do tworzenia i przechowywania kopii zapasowych i kopii bezpieczeństwa**

## Macierz dyskowa przeznaczona na kopie zapasowe i bezpieczeństwa

|  |  |  |
| --- | --- | --- |
| **Lp.** | Nazwa parametru | **Minimalna wartość parametru** |
|  | Obudowa  | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  |   | System musi zostać dostarczony w konfiguracji zawierającej minimum:- 12 dysków 4TB NL-SAS- zajmować maksymalnie 2U w szafie rackSystem musi ponadto wspierać dyski:- SSD: od 800GB do 15.3TB- SAS 10k od 900GB do 1800GB- NL-SAS od 4TB do 18TBSystem musi mieć możliwość rozbudowy do minimum 180 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami). Zamawiający dopuszcza rozwiązanie, które nie pozwala na taką rozbudowę w przypadku, gdy zostanie zaoferowany najwyższy z modeli macierzy skalowalny min do 500 dysków oraz pamięcią cache min 512GB.Macierz musi pozwalać i być przystosowana na rozbudowę do modelu NVME bez potrzeby wymiany dysków i kopiowania danych.  |
|  | Kontroler  | Dwa kontrolery wyposażone w nie mniej niż 8GB cache każdy.W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.  |
|  | Interfejsy  | Oferowana macierz musi posiadać minimum - 4 porty 16Gb FC z wkładkami SFP+ dającymi możliwość podłączenia do przełącznika SUN Cisco MDS9148S-16 działającym obecnie u Zamawiającego- 4 porty SAS 12 Gb/s do podłączenia półek dyskowychMożliwość rozbudowy lub wymiany do 12 portów 10GbE lub/i 8 portów 32Gb lub/i 8 portów 12Gb SS 10k |
|  | RAID  | Wsparcie dla RAID: 0, 1, 5, 6, 10Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.  |
|  | Obsługiwane protokoły  | FC, iSCSI, SAS, S3, CIFS, NFSZamawiający dopuszcza zrealizowanie protokołu CIFS, NFS i S3 za pomocą zewnętrznego oprogramowania typu Software Defined Storage.  |
|  | Inne wymagania  | Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris, HP HP-UX, IBM AIX, Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen.Macierz musi posiadać funkcjonalność klonowania danychMacierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, oraz po Ethernecie w trybie asynchronicznym system musi pozwalać na wykonanie do 32 jednoczesnych replikacji. Wsparcie producenta dla replikacji z istniejącą macierzą Fujitsu/ Eternus DX200 S5.Macierz musi posiadać możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning).Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji. Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID.Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD.Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dyskówWraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: - wydajności i opóźnień na wolumenach- wydajności I/Ops, MB/sMacierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.  Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: - Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter- VMware VASA- MicrosoftVirtual Disk Service (VDS)- Microsoft Virtual Shadow Service (VSS)- Oracle Enterprise Manager – monitoring zasobów macierzowych Zamawiający dopuszcza zaoferowania zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji np. w formie Software Defined storage. Macierz musi pozwalać na szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami. |
|  | Gwarancja i serwis  | 24 miesięcy serwisu producenta lub autoryzowanego partnera, zapewniającego dostawę podzespołu zapasowego na następny dzień roboczy od diagnozy problemu. Możliwość zgłaszania awarii poprzez linię telefoniczną lub inne systemy informatyczne producenta lub partnera.Dostarczony system musi posiadać również 36 miesięcy serwisu (aktualizacje i wsparcie) producenta dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.Zepsute dyski zostają u zamawiającego |

## Przełącznik FC do systemu kopi zapasowych i bezpieczeństwa

1. Zamawiający w swojej infrastrukturze obecnie wykorzystuje przełącznik Cisco MDS9148S-16.
2. Zamawiający wymaga by dostarczony przełącznik SAN był podłączony do obecnie działającego w sieci.
3. Urządzenie musi być wyposażone w nie mniej niż 16 aktywne porty Fibre Channel w standardzie SFP pracujące w trybie 2/4/8/16 Gbps z pełną przepustowością dla prędkości 16G FC.
4. Musi istnieć możliwość zwiększenia liczby aktywnych portów urządzenia do 48 portów 2/4/8,16G FC bez potrzeby rozbudowy sprzętowej, jednie poprzez aktywację na podstawie licencji.
5. 16 portów musi zostać obsadzonych wkładkami optycznymi wyposażonymi w interfejsy optyczne SW FC 16 GBps SW(short-wave);
6. Urządzenie musi być wyposażone w oprogramowanie umożliwiające uruchomienie, konfigurację oraz komunikację z działającą u Zamawiającego siecią SAN;
7. Każdy port musi być wyposażony w minimum 64 buffer credits
8. Przynajmniej jednak czwarta (25%) portów musi mieć możliwość wyposażenia w 250 kredytów.
9. Urządzenie musi wspierać podział sieci SAN na wirtualne sieci SAN (wirtualne fabryki);
10. Urządzenie musi umożliwiać dynamiczny przydział portów do wirtualnych sieci (fabryk) SAN
11. Urządzenie musi wspierać możliwość stworzenia, co najmniej 32 wirtualnych sieci (fabryk) SAN;
12. Urządzenie musi umożliwiać agregację nie mniej niż 16 portów fizycznych w jedno połączenie logiczne („trunk”, „channel“). Jeśli opisany mechanizm wymaga licencji musi być ona dostarczona razem z urządzeniem.
13. W skład zagregowanego połączenia logicznego („trunk”, „channel“) musi być możliwe włączenie dowolnego aktywnego portu przełącznika
14. Urządzenie musi wspierać wymianę oprogramowania bez przerwy w działaniu urządzenia (tzw. nondisruptive software upgrades);
15. Urządzenie musi posiadać możliwość wsparcia dla mechanizmów gwarancji jakości usług (QoS). Jeśli funkcjonalność do pracy potrzebuje dodatkowej licencji to nie jest wymagane dostarczenie jej na obecnym etapie postępowania.
16. Urządzenie musi umożliwiać definiowanie i dystrybucję aliasów dla WWNN
17. Urządzenie musi posiadać wsparcie dla następujących mechanizmów:
	1. Sprzętowo implementowany zoning,
	2. N-Port ID Virtualization (NPIV),
	3. Zarządzanie/monitorowanie SNMPv3,
	4. Dostęp administracyjny SSHv2,
	5. Transfer za pomocą SFTP,
	6. Autoryzacja dostępu administracyjnego do przełącznika za pomocą RADIUS i TACACS+, LDAP, Microsoft Active Directory;
	7. Mechanizmy ochrony warstwy control plane
18. Urządzenie musi zapewniać integrację z posiadanymi przez Zamawiającego przełącznikami SAN na bazie wirtualnych sieci (fabryk) SAN, zoningu oraz dystrybucji aliasów
19. Urządzenie musi posiadać możliwość konfiguracji poprzez terminal i linię komend CLI oraz interfejs graficzny GUI. Oprogramowanie do konfiguracji i monitorowania przełącznika, musi być wyposażone w graficzny interfejs użytkownika, o co najmniej następujących funkcjonalnościach:
	1. Konfiguracja parametrów pracy w wielu urządzeniach jednocześnie w obrębie pojedynczej sieci SAN,
	2. Wyświetlanie stanu poszczególnych portów i modułów,
	3. Wizualizacja topologii sieci SAN. Wizualizacja fizycznych połączeń między urządzeniami z podaniem informacji o łączach (przynajmniej stan, prędkość, typ),
	4. Wizualizacja statystyk poszczególnych portów i modułów;
	5. Konfiguracja całej sieci (fabryki) SAN oraz poszczególnych przełączników i ich portów
	6. Uproszczone narzędzia konfiguracyjne
	7. Narzędzia diagnostyczne łącznie analizą działania (fabryki) SAN w tym zjawiska slow-drain.
	8. Wizualizacja wydajności działania
	9. Wizualizacja błędów i alarmów
20. Urządzenie musi być wyposażone w szeregowy port konsoli.
21. Urządzenie musi być wyposażone w następujące narzędzia diagnostyczne
	1. Rejestrowanie zdarzeń poprzez mechanizm syslog,
	2. Możliwość bezzakłóceniowego monitorowania ruchu na portach przez kopiowanie ruchu z określonego portu na wybrany port monitorujący (z dołączonym zewnętrznym analizatorem),
	3. Narzędzia dla Fibre Channel odpowiadające fukcjonalnie poleceniom sieciowym „ping” i „traceroute”,
22. Urządzenie musi posiadać redundantne zasilacze z możliwością ich wymiany w czasie pracy
23. Urządzenie musi posiadać obudowę o maksymalnej wysokości 1RU (rack unit), przystosowaną do montażu w szafie 19” i wykonaną z metalu;
24. Urządzenie musi być objęte minimum 24 miesięczną gwarancją producenta obejmującą sprzęt, w tym oprogramowanie wbudowane zainstalowane na sprzęcie lub niezbędne do jego poprawnego funkcjonowania. Gwarancja musi umożliwiać:

- dostęp do całodobowej Infolinii producenta lub autoryzowanego przedstawiciela

- dostęp do poprawek i najnowszych wersji oprogramowania ze strony producenta lub autoryzowanego przedstawiciela i możliwość ich pobierania

## Wymagania ogólne wobec urządzeń, o których w pkt. 1 – 2 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. Wymagane jest, aby data produkcji dostarczonych urządzeń nie była wcześniejsza niż 12 miesięcy od daty ogłoszenia postępowania.

## System do backupu danych

Ilość dostarczonych licencji na oprogramowanie musi obejmować wszystkie działające u Zamawiającego serwery fizyczne oraz wirtualne. Zamawiający dysponuje 40 serwerami wirtualnymi uruchomionymi na platformie VMware uruchomionych na 4 serwerach fizycznych. Są to zarówno systemy Linuxowe, MS Windows Server 2022 oraz dwa serwery Oracle spięte w klastrze.

Wymagane jest dostarczenie kompletu licencji **bezterminowych** oprogramowania do tworzenia kopi zapasowych oraz bezpieczeństwa spełniającego poniższe wymagania minimalne:

1. Licencje muszą zostać objęte min 36 miesięcznym wsparciem producenta umożliwiającym pobieranie nowych wersji oprogramowania i zgłaszanie nieprawidłowości w funkcjonowaniu systemu.
2. 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.
3. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowe
4. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
5. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
6. 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
7. 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.
8. 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.
9. 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.
10. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
11. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
12. 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)
13. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
14. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
15. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
16. 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
17. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
18. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
19. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
20. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
21. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
22. 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
23. Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
24. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
25. 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.
26. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
27. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
28. Oprogramowanie musi posiadać wsparcie dla NDMP
29. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
30. 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.
31. 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.
32. 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)
33. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
34. 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.
35. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
36. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
37. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
38. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
39. 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)
40. 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
41. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
42. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
43. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
44. 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
45. 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.
46. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
	1. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
	2. BSD: UFS, UFS2
	3. Solaris: ZFS, UFS
	4. Mac: HFS, HFS+
	5. Windows: NTFS, FAT, FAT32, ReFS
47. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
48. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
49. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
50. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
51. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
52. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
53. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
54. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
55. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
56. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
57. 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.
58. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
59. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
60. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
61. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
62. 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.
63. 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
64. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
65. 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.
66. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
67. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
68. 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
69. 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.
70. System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
71. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
72. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
73. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
74. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
75. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
76. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
77. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
78. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
79. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
80. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
81. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
82. 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.
83. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
84. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x
85. Raportowanie
86. 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
87. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
88. System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
89. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
90. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
91. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
92. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
93. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
94. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
95. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
96. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
97. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
98. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
99. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
100. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
101. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
102. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

## Wymagania ogólne wobec licencji, o których mowa w pkt. 3 powyżej:

Zamawiający wymaga zapewnienia licencji zgodnie z następującymi minimalnymi wymaganiami, o ile w specyfikacji poszczególnych elementów zamówienia nie wymagano inaczej:

* + - 1. Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia (np.: certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, wpis na stronie producenta oprogramowania, itp.).
			2. Zamawiający nie dopuszcza dostawy licencji typu OEM.
			3. Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.
			4. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w działaniu środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem infrastruktury sprzętowo-programowej do stanu sprzed instalacji Oprogramowania oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.
			5. Licencje mają pozwalać na korzystanie z aktualizacji danego oprogramowania
			6. Licencje mają pozwalać na korzystanie z ukazujących się poprawek do danego oprogramowania.

## Wdrożenie systemu kopii zapasowych

Celem wdrożenia jest:

1. Stworzenie i przetestowanie systemu do tworzenie kopi zapasowych,
2. 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.
3. Instalacje i konfiguracje elementów systemu mają odbywać się zgodnie z najlepszymi praktykami przedstawianymi przez producentów poszczególnych urządzeń i oprogramowania.
4. 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.
5. 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
6. 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.
7. 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.

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.

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. Urządzenie 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.

6. Zamawiający wymaga konfiguracji dostarczonych serwerów zgodnie z wymaganiami Zamawiającego.

7. Zamawiający wymaga uruchomienia dostarczonych serwerów zgodnie z wymaganiami licencyjnymi zakupionego oprogramowania

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

9. Wdrożenie systemu do zarządzania zdarzeniami niepożądanymi musi obejmować wszystkie urządzenia aktywne całego systemu Zamawiającego.

## Szkolenia

Zamawiający wymaga przeprowadzenia szkoleń personelu Zespołu ds. Informatyki na poziomie eksperta z zakresy wdrożonych systemów tworzenia kopi zapasowych. Szkolenia obejmują 2 osoby.

## Specyfikacja gwarancyjnych usług serwisowych po instalacji, wdrożeniu i uruchomieniu:

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.

### **Pakiet 2**

## **System usług poczty elektronicznej**

## Serwer do usług poczty elektronicznej

|  |  |
| --- | --- |
| Obudowa | * Typu RACK, wysokość nie więcej niż 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Ramię porządkujące ułożenie przewodów z tyłu serwera;
* Możliwość zainstalowania 16 dysków twardych hot plug;
* Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
* Zainstalowane 2 szt. dysków SSD SATA 480GB – system RAID 10
* Zainstalowane 4 szt. dysków 4TB - dane
 |
| Płyta główna | * Dwuprocesorowa;
* Możliwość instalacji procesorów 38-rdzeniowych;
* Możliwość zainstalowania modułu TPM 2.0;
* 7 złącz PCI Express generacji 4 w tym:
	+ 4 fizyczne złącza o prędkości x16;
	+ 3 fizyczne złącza o prędkości x8;
	+ Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	+ Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
* 32 gniazda pamięci RAM;
* Obsługa minimum 4TB pamięci RAM DDR4;
* Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna
* Wsparcie dla technologii:
	+ Memory Scrubbing
	+ SDDC
	+ ECC
	+ Memory Mirroring
	+ ADDDC;
* 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)
* Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  nie zajmujące klatek dla dysków hot-plug;
 |
| Procesory | * 1 procesor 26-rdzeniowy
* Taktowanie 2.20GHz
* architektura x86\_64

osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 345 pkt  (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/cpu2017.html> |
| Pamięć RAM | * 512 GB pamięci RAM
* DDR4 Registered
* 3200Mhz
 |
| Kontrolery LAN | * Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 10Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
* Dodatkowa karta zainstalowane w slocie PCIe 2x 10Gbit SFP+, wszystkie porty obsadzone modułami MMF LC do współpracy z przełącznikiem Cisco MDS9148S-16 który obecnie działa u Zamawiającego.
 |
| Kontrolery I/O | * Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug;
* Zainstalowany wewnętrzy kontroler SAS RAID obsługujący poziomy 0,1,10,5,50 obsługujący zaoferowane dyski twarde;
* Dodatkowa dwuportowa karta FC 16G zainstalowana w slocie PCIe, wszystkie porty typu MMF LC zgodna z dostarczonym w ramach tego postępowania przełącznikiem FC.
 |
| Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
* 2 port USB 3.0 wewnętrzne;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* 2 porty USB-C lub 2 porty USB-A 3.0 lub 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% (tzw. klasa Platinum) o mocy minimalnej 900W;
* Redundantne wentylatory hotplug;
 |
| Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii
	+ informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
		- karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express
		- procesory CPU
		- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
		- wbudowany na płycie głównej nośnik pamięci M.2 SSD
		- status karty zrządzającej serwera
		- wentylatory
		- bateria podtrzymująca ustawienia BIOS płyty główne
		- zasilacze

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
	+ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	+ Dostęp poprzez przeglądarkę Web, SSH;
	+ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	+ Zarządzanie alarmami (zdarzenia poprzez SNMP)
	+ Możliwość przejęcia konsoli tekstowej
	+ Możliwość zarządzania przez 6 administratorów jednocześnie
	+ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
	+ Obsługa serwerów proxy (autentykacja)
	+ Obsługa VLAN
	+ Możliwość konfiguracji parametru Max. Transmission Unit (MTU)
	+ Wsparcie dla protokołu SSDP
	+ Obsługa protokołów TLS 1.2, SSL v3
	+ Obsługa protokołu LDAP
	+ Integracja z HP SIM
	+ Synchronizacja czasu poprzez protokół NTP
	+ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
* Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
* Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
* Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
* BIOS UEFI w specyfikacji 2.7;
 |
| 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 producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu lub autoryzowanego partnera 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;
 |
| Dokumentacja, inne | * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
* Telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii 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 strony www producenta serwera;
* Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
* Zgodność z normami: CB, RoHS, WEEE, GS oraz CE;
 |

## Wymagania ogólne wobec urządzenia, o których w pkt. 1 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.

Wymagane jest, aby data produkcji dostarczonych urządzeń nie była wcześniejsza niż 12 miesięcy od daty ogłoszenia postępowania.

## System do wirtualizacji

Wymagane jest dostarczenie 1 szt. licencji oprogramowania 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.

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, 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. 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.

## Wymagania ogólne wobec licencji, o których mowa w pkt. 2 powyżej:

Zamawiający wymaga zapewnienia licencji zgodnie z następującymi minimalnymi wymaganiami, o ile w specyfikacji poszczególnych elementów zamówienia nie wymagano inaczej:

1. Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia (np.: certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, wpis na stronie producenta oprogramowania, itp.).

2. Zamawiający nie dopuszcza dostawy licencji typu OEM.

3. Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.

4. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w działaniu środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem infrastruktury sprzętowo-programowej do stanu sprzed instalacji Oprogramowania oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.

5. Licencje mają pozwalać na korzystanie z aktualizacji danego oprogramowania

6. Licencje mają pozwalać na korzystanie z ukazujących się poprawek do danego oprogramowania.

## Zaprojektowanie systemu poczty elektronicznej, uruchomienie i przeniesienie wszystkich obecnych danych.

Zamawiający wymaga zakupu, dostarczenia serwera oraz zaplanowania, przygotowania i wdrożenia systemu do obsługi poczty elektronicznej Zamawiającego. Oprogramowanie musi być uruchomione na wirtualnym serwerze wskazanym przez Zamawiającego. Jeżeli Wykonawca uzna iż do tych zadań przygotowane rozwiązanie jest niewystarczające powinien to zgłosić Zamawiającemu na etapie planowania.

Zamawiający wymaga by systemem operacyjnym na którym będą uruchomione kolejne elementy systemu pocztowego był Linux. Pakiety wchodzące w skład oprogramowania muszą tworzyć grupę aplikacji spełniająca wszystkie potrzeby Zamawiającego. Obowiązkowymi elementami całego narzędzia do obsługi poczty elektronicznej muszą być:

1. system MTA typu Postfix, oprogramowanie do wymiany poczty elektronicznej za pośrednictwem protokołu SMTP. Wykonawca musi zaproponować najbardziej odpowiedni skład tych modułów. System musi współpracować z oprogramowaniem bazodanowym zawartym w dystrybucji systemu, gdzie przechowywane są informacje o kontach użytkowników np. MsSQL, MariaDB lub PostgreSQL.
2. oprogramowanie typu Amavis, Spamassassin, służące do zabezpieczenia serwera poczty elektronicznej opartej o Linux przed SPAM’em. Dający możliwość przygotowania odpowiedniej kombinacji filtrów umożliwiające blokowanie niechcianej poczty. Narzędzie to musi umożliwiać testowanie każdej wiadomości przed dostarczeniem do użytkownika. Jeśli zostanie spełniony określony warunek naliczane są punktu. Po sprawdzeniu wszystkich reguł punkty są sumowane, jeśli przekroczą określony pułap poczta klasyfikowana jest jako SPAM. Narzędzie to musi także wykorzystać komercyjne lub darmowe filtry antyspamowe i antywirusowe jak na przykład CISCO ESA – IronPort.
3. oprogramowanie typu Dovecot, obsługujące protokoły POP/IMAP, służące do odbioru poczty elektronicznej przez aplikacje klienckie . Tak jak Postfix, Dovecot posiada bogatą konfigurację oraz potrafi współpracować z aplikacjami zewnętrznymi w tym bazami danych, gdzie może być przechowywana konfiguracja użytkowników. System MTA oraz Dovecot posiadają moduły umożliwiające współpracę np. w obszarze autoryzacji użytkowników.
4. oprogramowanie typu Roundcube czy Modoboa, daje możliwość korzystania z poczty elektronicznej przez interfejs WWW. Aplikacja te posiadają szereg rozszerzeń, które Wykonawca w trakcie planowania może zaproponować Zamawiającemu jako bardziej optymalne.
5. oprogramowanie umożliwiające przesyłanie na odpowiednie konta administratorów informacji o:
	1. utworzeniu nowego konta
	2. zmianie już istniejącego konta
	3. innych informacji niezbędnych do prawidłowego zrządzania systemem poczty elektronicznej
6. Zamawiający wymaga sprawdzenia poprawności działania całego systemu podtrzymania zasilania UPS w tym również systemu poczty elektronicznej.
	1. Sprawdzenie ma obejmować prawidłowość obciążenia poszczególnych UPS’ów
	2. Możliwość uruchomienia komunikacji z wykorzystaniem modułów LAN
	3. Stanu zużycia akumulatorów w tych UPS’ach

## Wymagania dotyczące licencji

Zamawiający wymaga zapewnienia licencji zgodnie z następującymi minimalnymi wymaganiami, o ile w specyfikacji poszczególnych elementów zamówienia nie wymagano inaczej:

1. Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia (np.: certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, wpis na stronie producenta oprogramowania, itp.).
2. Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.
3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w działaniu środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem infrastruktury sprzętowo-programowej do stanu sprzed instalacji Oprogramowania oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.
4. Licencje mają pozwalać na korzystanie z aktualizacji danego oprogramowania.
5. Licencje mają pozwalać na korzystanie z ukazujących się poprawek do danego oprogramowania.

W przypadku gdy Wykonawca zaproponuje licencje odpłatne Zamawiający wymaga zabezpieczenia 36 miesięcznego okresu wsparcia ze strony producenta oprogramowania lub autoryzowanego partnera.

## Wdrożenie

1. Bezpieczne zmodernizowanie, przeniesienie i produkcyjne uruchomienie na nowej platformie obecnie działającej poczty elektronicznej,
2. Zamawiający wymaga migracji wszystkich danych z obecnie działających serwerów poczty elektronicznej do nowych zgodnie z uzgodnieniami dokonanymi z Zamawiającym. W ramach umowy Wykonawca w uzgodnionym z Zamawiającym terminie dokona migracji w taki sposób, aby wszystkie materiały i pliki były dostępne dla użytkowników końcowych w trakcie wykonywania migracji. Jeśli z przyczyn technicznych migracja online dla wybranego zasobu będzie niedostępna Wykonawca uzgodni z Zamawiającym termin i czas niedostępności zasobu (np. godziny nocne, sobota).
3. Wykonawca zapewni przez okres pierwszy 7 dni od produkcyjnego uruchomienia systemu możliwość szybkiego wsparcia w trakcie sytuacji awaryjnej. Przez sytuacje awaryjna Zamawiający rozumie zatrzymanie jakiejkolwiek z usług serwera poczty elektronicznej, nie przekazywanie wiadomości do skrzynek użytkowników, brak możliwości zalogowania się do skrzynek przez użytkowników.

## Szkolenia

1. Zamawiający wymaga przeszkolenia dwóch administratorów w zakresie:
	1. Monitorowania pracy całego systemu,
	2. Pobieranie i uruchamianie aktualizacji systemu na którym uruchomiony jest system poczty elektronicznej,
	3. Pobierania i uruchamiania aktualizacji poszczególnych modułów,
	4. Tworzenia kont dla nowych użytkowników,
	5. Tworzenia aliasów do poszczególnych kont i użytkowników,
	6. Modyfikacji już istniejących kont
	7. Modyfikacja i tworzenie nowych filtrów do poczty
	8. Tworzenie nowych i modyfikowania działających zabezpieczeń systemu poczty elektronicznej

## Specyfikacja usług gwarancyjnych oraz usług wsparcia technicznego

1. W ramach udzielonej gwarancji i wsparcia technicznego Wykonawca zapewni pełną funkcjonalność systemu w skład którego wchodzą dostarczone urządzenie i oprogramowanie wraz z pakietami - poprzez bezpłatne usuwanie awarii, usterek i wad dostarczonych urządzeń, dostarczanie nowych wersji oprogramowania oraz udzielanie bezpłatnych konsultacji.

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. 6 godziny od momentu zaewidencjonowania zgłoszenia serwisowego przez Użytkownika Zamawiającego.

6. Użytkownik Zamawiającego będzie miał możliwość zaewidencjonować następujące rodzaju zgłoszenia:

6.1. awaria - oznacza sytuację, w której nie jest możliwe prawidłowe używanie części lub całości uruchomionego systemu.

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. Konsultacje

Zasady świadczenia usług – tabela skrócona:

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Rodzaj świadczonych usług | Czas wykonania zlecenia serwisowego | Warunki świadczenia usług |
| 1. | Awaria  | czas usunięcia – 6 h  | Czas liczony w godzinach od upływu czasu reakcji serwisu Wykonawcy do momentu usunięcia awarii. |
| 2. | 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 wsparcia technicznego. |

Szczegółowy zakres oraz warunki realizacji usług:

1. Awaria

1.1. Czas usunięcia awarii - maksymalnie 6 godzin od upływu czasu reakcji serwisu Wykonawcy do godziny całkowitego usunięcia awarii i wykonania przez Wykonawcę testu poprawnego działania systemu, zaakceptowanego przez Zamawiającego.

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

1.3. Zgłoszenie serwisowe jest ostatecznie zamykane jeżeli upłynęło 7 dni od terminu usunięcia Awarii i wykonania testu systemu zaakceptowanego przez Zamawiającego, a Zamawiający nie wniósł w tym czasie zastrzeżeń do wyniku.

2. Konsultacja

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

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

2.1.2. 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.

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

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

Po upływie 7 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