

Opis Przedmiotu Zamówienia

Zakup wsparcia producenta dla infrastruktury HPE i oprogramowania do wykonywania backupu oraz dostawa subskrypcji dla systemu wirtualizacji

Przedmiotem zamówienia jest zakup pełnego wsparcia producenta na posiadany sprzęt HPE Synergy 12000 w infrastrukturze uniwersalnej i na posiadane oprogramowanie Veeam Backup&Replication oraz dostawa subskrypcji oprogramowania do wirtualizacji.

Przedmiot zamówienia w szczególności obejmuje 3 zadania:

1. Zadanie I – zapewnienie pełnego wsparcia producenta dla posiadanego sprzętu HPE w Uniwersalnej infrastrukturze sprzętowo-programowej.
2. Zadanie II –zapewnienie wsparcia producenta dla posiadanego oprogramowania do backupu Veeam Backup&Replication i pakietu do monitorowania infrastruktury wirtualizacyjnej Veeam Management Pack for System Center Operation Manager, lub dostawa równoważnego oprogramowania
3. Zadanie III – Dostawa subskrypcji oprogramowania do wirtualizacji.

Rozdział I

Uwarunkowania realizacji zadań oraz opis posiadanej przez Zamawiającego infrastruktury

Wszystkie prace będą realizowane w siedzibie Zamawiającego tj. serwerowniach Centrum Informatyki Statystycznej mieszczących się w budynku Głównego Urzędu Statystycznego przy al. Niepodległości 208 w Warszawie i będą odbywać się pod nadzorem administratorów Centrum Informatyki Statystycznej.

Z uwagi na fakt, iż prace będą prowadzone w działającym środowisku sprzętowo-systemowo-aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska. W przypadku, w którym nie jest możliwe wykonanie przedmiotu zamówienia bez zapewnienia ciągłości działania środowiska dopuszcza się minimalne przestoje. Wszelkie przestoje i wyłączenia wymagają akceptacji Zamawiającego. Konieczność przestoju musi być zgłoszona przez Wykonawcę z wyprzedzeniem 4 dni roboczych. Zamawiający zastrzega sobie prawo do odmowy wykonania przestoju w środowisku oraz/lub wyznaczenia własnego terminu przestoju.

1. Bezpieczeństwo łańcucha dostaw i zarządzanie dostawcami

Wykonawca zobowiązuje się do zapewnienia bezpieczeństwa, zgodnie z wymogami Dyrektywy (UE) 2022/2555 (NIS2).

2. Wykonawca przedstawi Zamawiającemu listę bezpośrednich dostawców komponentów sprzętowych i programowych wykorzystywanych w realizowanych zadaniach, wraz z:

- a) nazwą dostawcy,
- b) zakresem dostarczanych komponentów lub usług,
- c) wersjami oprogramowania i datami wsparcia technicznego,
- d) informacjami o stosowanych licencjach (w tym komponenty Open Source).

3. W przypadku wykrycia podatności lub naruszenia bezpieczeństwa przez podwykonawcę, Wykonawca zobowiązuje się do niezwłocznego powiadomienia Zamawiającego.

4. Wykonawca stosuje zasady Zero Trust.

5. Wykonawca zapewnia, że wszystkie komponenty sprzętowe i programowe spełniają aktualne wymagania bezpieczeństwa.

Ogólny opis Infrastruktury sprzętowo-programowej oraz licencji oprogramowania posiadanych przez Zamawiającego

Dla poszczególnych zadań należy przyjąć podane poniżej liczby posiadanych przez Zamawiającego elementów infrastruktury:

Zadanie I

1. 3 zestawy infrastruktury serwerowo-sieciowych HPE Synergy 12000 Frame (w każdym po 3 obudowy blade) oraz moduły pamięci masowej HPE Synergy D3940 z dyskami SSD wraz z infrastrukturą towarzyszącą;
2. system usług katalogowych bazujący na MS Active Directory w wersji Windows Server 2019 o funkcjonalności lasu i domeny na poziomie wersji Windows Server 2012 R2;
3. wieczyste licencje VMware Cloud Foundation Advanced 5 z funkcjonalnościami NSX i vSAN, vRealize Network Insight, vRealize Suite, SDDC Manager for VCF oraz vCenter Server 8.0.2;
4. wieczyste licencje Veeam Backup&Replication.

Szczegółowy wykaz infrastruktury dla Zadania I jest przedstawiony w tabeli w załączniku nr 1 do OPZ ma charakter poufny. Udostępnienie tych informacji opisane zostało w pkt 3 rozdziału III SWZ. Wykonawca zobowiązany jest do zachowania poufności oraz do nieudostępniania osobom trzecim otrzymanych informacji.

Zadanie II i III

1. 3 zestawy infrastruktury serwerowo-sieciowych HPE Synergy 12000 Frame (w każdym po 3 obudowy blade) oraz moduły pamięci masowej HPE Synergy D3940 z dyskami SSD wraz z infrastrukturą towarzyszącą;
2. 36 serwerów HPE SY 480 Gen10 dwuprocesorowych (20 i 8-rdzeniowych);
3. System usług katalogowych bazujący na MS Active Directory w wersji Windows Server 2019 o funkcjonalności lasu i domeny na poziomie wersji Windows Server 2012 R2;
4. Wieczyste licencje VMware Cloud Foundation Advanced 5.1 z funkcjonalnościami NSX i vSAN, vRealize Network Insight, vRealize Suite, SDDC Manager for VCF oraz vCenter Server 8.0.2;
5. Zamawiający posiada wieczyste licencje Veeam Backup&Replication:
 - 1) oprogramowanie do tworzenia kopii zapasowych Veeam Backup&Replication Enterprise Plus: 60 Sockets - Contract 03547420 aktywny do dnia 30.11.2025r.; 12 Sockets - Contract 02279316 aktywny do dnia 04.11.2025 r,
 - 2) pakietu do monitorowania infrastruktury wirtualizacyjnej Veeam Managemant Pack for System Center Operation Manager: 60 Sockets - Contract 03547421 aktywnego do dnia 20.12.2025 r; 12 Sockets - Contract 02279317 aktywnego do dnia 04.11.2025r.;

Rozdział II

Zadanie I. Zapewnienie pełnego wsparcia producenta dla posiadanego sprzętu HPE w Uniwersalnej Infrastrukturze sprzętowo-programowej na okres 12 miesięcy od daty podpisania umowy, w tym 30 dni na uruchomienie usługi.

I. Realizacja Zadania I

1. Wykonawca wyznaczy koordynatora kontraktu w celu dokonywania wszelkich uzgodnień w zakresie realizacji przeglądów, aktualizacji i napraw urządzeń.
2. Wykonawca zakupi dla Zamawiającego pełne wsparcie producenta w ramach jednej standardowej usługi (która będzie w sobie zawierać pozostawienie uszkodzonych dysków u zamawiającego) na sprzęt HPE wymieniony w załączniku 1 na okres 12 miesięcy od daty podpisania umowy, w tym 30 dni na uruchomienie usługi, w przypadku pojedynczych urządzeń do wejścia w status „end of life”u producenta dla urządzenia którego ten status dotyczy.
3. Udostępnienie załącznika nr 1 do OPZ opisane zostało w pkt 3 rozdziału III SWZ.
4. W ramach usługi wsparcia producenta musi być zapewniony dostęp do supportu producenta dla Zamawiającego.
5. W ramach usługi wsparcia musi być zapewniony monitoring z powiadamianiem suportu producenta infrastruktury wymienionej w załączniku 1.
6. Support Wykonawcy świadczony w ramach usługi wsparcia musi być dostępny 24h na dobę, 7 dni w tygodniu.
7. W ramach usługi wsparcia producenta muszą być wykonywane dla Zamawiającego analizy logów

i diagnoza infrastruktury wymienionej w załączniku 1 oraz muszą być usuwane wszystkie zgłoszone awarie, błędy, ostrzeżenia i problemy dotyczące infrastruktury wymienionej w załączniku 1 w tym oprogramowania monitorującego i zarządzającego np.: HPE OneView, HPE OneView Global Dashboard, ILO.

8. W ramach usługi wsparcia muszą być naprawione wszystkie zgłoszone przez Zamawiającego usterki, błędy i ostrzeżenia będące skutkiem prac serwisu producenta lub wadliwego działania dostarczonych przez niego podzespołów i urządzeń.
9. Serwis producenta lub Wykonawca wykona wszystkie konfiguracje, aktualizacje i instalacje konieczne do usunięcia awarii i rozwiązania problemu zgłoszonego przez Zamawiającego.
10. W przypadku zgłoszenia awarii do Wykonawcy i konieczności naprawy komponentu sprzętowego wymienionego z załączniku 1 Wykonawca zobowiązany jest do zgłoszenia naprawy do serwisu producenta sprzętu.
11. Wykonawca musi współpracować z supportem producenta infrastruktury Zamawiającego przy usuwaniu awarii i aktualizacjach.
12. Serwis producenta podczas naprawy związanej z wymianą komponentu sprzętowego musi dostarczyć komponent o takich samych lub nie gorszych parametrach jakie miał komponent wymieniany oraz o takich które nie pogorszą działania urządzenia.
13. Wszystkie użyte do naprawy komponenty muszą być fabrycznie nowe, nieużywane, pochodzące z oficjalnych kanałów dystrybucji producenta a w przypadku niedostępności na rynku identycznych komponentów nowe muszą być dedykowane przez producenta infrastruktury opisanej w załączniku 1 do użycia w miejscu ich montażu.
14. Wymiana komponentu sprzętowego wykonywana będzie w siedzibie Zamawiającego. Termin wymiany musi być uzgodniony z Zamawiającym.
15. Serwis producenta podejmie działania mające na celu wymianę uszkodzonych podzespołów infrastruktury objętej wsparciem muszą rozpocząć się w terminie nie dłuższym niż 3 dni zawarte w przedziale poniedziałek-piątek liczone od daty zgłoszenia.
16. Serwis producenta podejmie działania mające na celu usunięcie usterek, błędów, ostrzeżeń i awarii zgłoszonych przez Zamawiającego muszą się rozpocząć w terminie nie dłuższym niż 3 dni zawarte w przedziale poniedziałek-piątek liczone od daty zgłoszenia.
17. Serwis producenta dokona rozpoczęcia naprawy zgłoszonych przez Zamawiającego usterek, błędów i ostrzeżeń będących skutkiem prac serwisu lub wadliwego działania dostarczonych przez niego podzespołów w ciągu 3 dni zawartych w przedziale poniedziałek-piątek od daty zgłoszenia przez Zamawiającego.
18. Wszelkie koszty związane z naprawami w okresie obowiązywania umowy włączając w to koszt komponentu sprzętowego, transportu do i z siedziby Zamawiającego, aktualizacji i instalacji oprogramowania, sterowników, firmware oraz koniecznych do wykonania w ramach zgłoszenia konfiguracji w środowisku Zamawiającego ponosi Wykonawca.
19. W przypadku wymiany dysku magnetycznego lub SSD na nowy, uszkodzony dysk zostaje własnością Zamawiającego i nie może opuszczać siedziby Zamawiającego. Koszt wymiany dysków ponosi Wykonawca.
20. Jeśli po wymianie komponentu sprzętowego pojawią się błędy lub ostrzeżenia (np. w HPE OneView, HPE OneView Global Dashboard, ILO) to serwis producenta musi je naprawić bezpośrednio po ich pojawieniu się.
21. Po zakończeniu naprawy środowisko infrastruktury sprzętowo-programowej Zamawiającego musi posiadać wszystkie funkcjonalności i komponenty działające w sposób nie gorszy jak przed wykonaniem naprawy.
22. W przypadku wymiany dysku w kasetach HPE D3940, Wykonawca musi doprowadzić do stanu takiego, że wymieniony dysk jest poprawnie prezentowany (to znaczy w taki sam sposób i w tych samych miejscach jak dysk podlegający wymianie) dla serwera, do którego jest przypisany oraz jest poprawnie rozpoznawany w OneView jako logical JBOD do Server Template odpowiedniego serwera a profil serwera do którego jest przypisany ma status „Konsystentny”. Server Template, Server Profiles, logical JBOD, OneView muszą prezentować poprawną pracę (bez ostrzeżeń i

- alertów) wymienionego dysku. W internetowym systemie serwisowanym HPE jest widoczna dla niego informacja o statusie i długości terminu gwarancji.
23. Zamawiający wymaga, żeby Wykonawca lub serwis producenta podczas wykonywania naprawy dostarczył do siedziby Zamawiającego wszystkie komponenty potrzebne do wykonania naprawy osobiście oraz osobiście odebrał komponenty uszkodzone w terminie ustalonym z Zamawiającym. Zamawiający nie dopuszcza sytuacji w której musi na własną rękę odbierać komponenty niezbędne do wykonania naprawy i odsyłać komponenty uszkodzone.
 24. Zamknięcie zgłoszenia awarii przez Wykonawcę lub serwis producenta może zostać wykonane tylko po uzyskaniu zgody Zamawiającego.
 25. Wykonawca wraz z uruchomieniem usługi z zadania 1 pkt.2 uruchomi kanał kontaktowy umożliwiający zgłaszanie awarii w formie elektronicznej przez stronę www (portal zgłoszeniowy), w przypadku awarii portalu Zamawiający będzie mógł dokonać zgłoszenia za pomocą poczty elektronicznej lub za pomocą telefonu.
 26. Portal zgłoszeniowy musi przechowywać pełną historię zgłoszeń Zamawiającego zawierającą co najmniej datę i czas zgłoszenia, temat naprawy, osobę zgłaszającą, datę i czas wykonanej naprawy.
 27. Wykonawca w ramach usługi pełnego wsparcia producenta zapewni przez cały czas trwania umowy i usługi wsparcia producenta dostęp do stron www producenta w celu:
 - a) przeszukiwania bazy wiedzy producenta dotyczącej sprzętu objętego wsparciem technicznym;
 - b) uzyskiwania informacji o statusie Umowy oraz o sprzęcie nią objętym. Procedury dotyczące dokonywania zgłoszeń serwisowych, statusu napraw, opis procedury śledzenia zgłoszenia i eskalacji;
 - c) pobrania aktualnych wersji oprogramowania oraz krytycznych poprawek komponentów związanych z bezpieczeństwem i stabilnością działania oprogramowania w całym czasie trwania umowy. Poprzez oprogramowanie rozumie się stabilne wersje firmware, sterowników sprzętowych niezbędne dla prawidłowego działania komponentów i inne oprogramowanie wchodzące w skład infrastruktury wymienionej w załączniku 1. Wszelkie firmware i oprogramownie oraz podzespoły używane do realizowania zapisów niniejszego OPZ musi pochodzić z oficjalnego legalnego źródła producenta.
 - d) Zamawiający musi posiadać dostęp do portalu producenta sprzętu, który umożliwi zgłaszanie awarii bezpośrednio do producenta sprzętu.
 28. Wykonawca musi wykonać co najmniej 1 pełną aktualizację oprogramowania (w tym oprogramowania monitorującego i zarządzającego np.: One View, One View Global Dashboard, ILO), sterowników i firmware wszystkich komponentów wymienionych w załączniku 1 w okresie trwania umowy. Aktualizacje będą wykonywane na polecenie Zamawiającego w terminie do 30 dni zawartych w przedziale poniedziałek-piątek od zgłoszenia przez Zamawiającego. Pełna aktualizacja musi być zakończona nie później niż 30 kwietnia 2026.
 29. W pulę 1 pełnej aktualizacji opisanej w zadaniu 1 ppkt.28 nie wliczają się aktualizacje usuwające podatności krytyczne. Te muszą być instalowane na życzenie Zamawiającego w terminie do 10 dni zawartych w przedziale poniedziałek-piątek od zgłoszenia. Zamawiający zastrzega sobie prawo do wydłużenia tego okresu.
 30. Wykonawca na potrzeby aktualizacji musi każdorazowo przed aktualizacją wykonać analizę zgodności firmware, oprogramowania i hardware podlegających aktualizacji z tabelami zgodności producenta. Cały proces aktualizacji musi być zgodny z tabelami zgodności producenta co do wersji urządzeń, firmware oraz innego oprogramowania.
 31. Wykonawca w przypadku konieczności wykonywania aktualizacji zobowiązany jest do ustalenia z Zamawiającym terminu rozpoczęcia działania oraz przedstawienia harmonogramu wykonywania poszczególnych operacji uwzględniający kolejność wykonywania aktualizacji, restartów urządzeń oraz ewentualnych przestojów.
 32. Wykonawca może przystąpić do wykonania aktualizacji tylko wtedy gdy uzyska akceptację Zamawiającego przesłaną drogą elektroniczną.
 33. Wykonawca po wykonaniu aktualizacji powiadamia Zamawiającego również drogą elektroniczną.

34. Zamawiający wymaga aby po wykonaniu aktualizacji środowisko infrastruktury sprzętowo-programowej posiadało wszystkie funkcjonalności i komponenty działające w sposób nie gorszy jak przed wykonaniem aktualizacji.
35. Zamawiający dopuszcza wykonanie aktualizacji przez inżynierów wykonawcy, pod warunkiem zastosowania się do wszelkich procedur producenta dotyczących aktualizacji danego urządzenia.
36. Zamawiający zastrzega sobie prawo do wykonania aktualizacji we własnym zakresie, nie będzie to wliczone do puli 1 pełnej aktualizacji jakie powinien przeprowadzić Wykonawca.
37. Każde użyte do aktualizacji oprogramowanie, sterowniki, firmware muszą pochodzić z oficjalnych kanałów dystrybucji producenta infrastruktury opisanej w załączniku 1.
38. Wszelkie koszty związane z aktualizacjami ponosi Wykonawca.

II. Warunki gwarancji dla Zadania I

1. Wykonawca obejmie gwarancją świadczone bezpośrednio przez siebie usługi i wykonane prace opisane w Zadaniu I
2. Wykonawca w ramach gwarancji jest zobowiązany do naprawy wszelkich błędów, ostrzeżeń, awarii jakie pojawią się w następstwie jego prac. Prace mające na celu naprawę błędów, ostrzeżeń, awarii powinny się rozpocząć w ciągu 1 dnia zawartego w przedziale poniedziałek-piątek od czasu zgłoszenia przez zamawiającego.
3. Wykonawca w okresie obowiązywania umowy będzie świadczył usługi asysty technicznej dla środowiska sprzętowo – systemowo - aplikacyjnego opisanego w załączniku 1, w wymiarze 200 godzin. W ramach asysty technicznej Wykonawca będzie udzielał porad, analiz i rozwiązywał problemy zgłaszane przez Zamawiającego, dokonywał instalacji poprawek, patch-y i rekonfiguracji infrastruktury opisanej w załączniku 1.
4. Wszelkie aktualizacje, naprawy, analizy wchodzące w zakres Zadania I nie będą wliczane do puli godzin asysty technicznej.
5. Godziny asysty technicznej będą mogły być wykorzystane jedynie na zgłoszenie Zamawiającego. Zamawiający nie dopuszcza możliwości samodzielnego wykorzystywania przez Wykonawcę puli godzin asysty technicznej.
6. Wykonawca wykona prace w ramach asysty technicznej w ciągu maksymalnie 5 dni roboczych od czasu zgłoszenia przez Zamawiającego.
7. Wykonanie godzin asysty technicznej aż do ich wyczerpania będzie potwierdzane zbiorczym protokołem odbioru godzin asysty technicznej.
8. Do wykonywania wszystkich zgłoszeń przez Zamawiającego dotyczących gwarancji i godzin asysty technicznej Wykonawca udostępni internetowy portal zgłoszeniowy dostępny z przeglądarek internetowych Zamawiającego oraz adres email i numer telefonu.
9. Portal zgłoszeniowy i email do wykonywania zgłoszeń przez Zamawiającego muszą być dostępne dla Zamawiającego 24 godziny na dobę, 7 dni w tygodniu, oraz numer telefonu, który musi być dostępny od poniedziałku do piątku z wyłączeniem świąt w godzinach od 8:00 do 16:00 do wykonywania zgłoszeń przez Zamawiającego.
10. Wszelkie zgłoszenia wykonane przez Zamawiającego w tym godziny asysty technicznej niezależnie od sposobu zgłoszenia muszą być rejestrowane w portalu zgłoszeniowym Wykonawcy, posiadać indywidualny numer, indywidualną nazwę użytkownika wykonującego zgłoszenia i odpowiadającego na nie, treść zgłoszenia i odpowiedzi. Godziny asysty technicznej w internetowym portalu zgłoszeniowym muszą być rejestrowane osobno od innych zgłoszeń i w sposób pozwalający na łatwe ich policzenie.
11. Wszelkie zgłoszenia w portalu zgłoszeniowym muszą być dostępne co najmniej przez cały okres trwania umowy.

Rozdział III

Zadanie II - Zakup wsparcia na oprogramowanie do backup-u Veeam Backup&Replication i pakietu do monitorowania infrastruktury wirtualizacyjnej Veeam Management Pack for System Center Operation Manager.

Przedmiotem zamówienia jest zakup wsparcia producenta na posiadany system do tworzenia kopii zapasowych Veeam Backup&Replication Enterprise Plus (72 Sockets) i posiadane oprogramowanie - pakiet do monitorowania infrastruktury wirtualizacyjnej Veeam Management Pack for System Center Operation Manager (72 Sockets) w Uniwersalnej infrastrukturze sprzętowo-programowej Zamawiającego.

I. Realizacja Zadania II

1. Wykonawca zakupi wsparcie producenta dla wymienionego w „Ogólnym opisie Infrastruktury sprzętowo-programowej oraz licencji oprogramowania posiadanych przez Zamawiającego” (strona 2), posiadanego przez Zamawiającego oprogramowania Veeam, na poziomie Basic, na okres do 36 miesięcy:
2. - dla oprogramowania do tworzenia kopii zapasowych Veeam Backup&Replication Enterprise Plus: 60 Sockets; 12 Sockets
3. - dla pakietu do monitorowania infrastruktury wirtualizacyjnej Veeam Management Pack for System Center Operation Manager: 60 Sockets ; 12 Sockets;
4. Wykonawca w ramach usługi wsparcia producenta zapewni dostęp do stron www producenta w celu pobrania aktualnych wersji oprogramowania oraz krytycznych poprawek komponentów związanych z bezpieczeństwem i stabilnością działania oprogramowania w całym czasie obowiązywania wsparcia.
5. W ramach usługi wsparcia producenta musi być zapewniony dostęp do supportu producenta dla Zamawiającego.
6. Portal zgłoszeniowy producenta oprogramowania musi przechowywać pełną historię zgłoszeń Zamawiającego, zawierającą co najmniej datę i czas zgłoszenia, temat naprawy, osobę zgłaszającą, datę i czas zamknięcia zgłoszenia.
7. Zamknięcie zgłoszenia awarii przez Wykonawcę lub serwis producenta może zostać wykonane tylko po uzyskaniu zgody Zamawiającego.

II. Rozwiązania równoważne

Zamawiający dopuszcza składanie ofert równoważnych w rozumieniu art. 99 ust. 5 ustawy Pzp. W przypadku zaoferowania rozwiązania równoważnego na Wykonawcy spoczywa obowiązek wykazania jego równoważności. Przez produkt równoważny rozumie się taki, który w sposób poprawny współpracuje z posiadanym przez Zamawiającego oprogramowaniem i infrastrukturą, a jego zastosowanie nie wymaga żadnych nakładów po stronie Zamawiającego, związanych z dostosowaniem systemów i aplikacji do produktu równoważnego. **Produkt równoważny musi posiadać wszelkie funkcjonalności oprogramowania, opisane w pkt. 1 i 2 (poniżej)**

Wskazane w opisie nazwy produktów odnoszą się do posiadanego i wykorzystywanego przez jednostki organizacyjne służb Statystyki Publicznej oprogramowania, a zachowanie parametrów określonych jako równoważne jest konieczne do zachowania kompatybilności i spójności środowiska. Zamawiający oczekuje ofert spełniających wymagania minimalne określone poniżej:

1. Produkt równoważny dla posiadanego oprogramowania Veeam Backup&Replication Enterprise Plus.

1.1 W ramach prac wdrożeniowych Wykonawca:

- 1) Przygotuje szczegółowy **Projekt techniczny** realizacji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczanego oprogramowania oraz zawierający opis konfiguracji środowiska.
- 2) Wykona instalację i konfigurację wszystkich elementów oprogramowania wymaganych przez Zamawiającego.
- 3) Skonfiguruje infrastrukturę do backupu (repozytoria, biblioteki LTO i pozostałe elementy) i uruchomi tak aby była w pełni funkcjonalna we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania, zgodnie z Projektem technicznym.

- 4) Zmigruje pliki kopii zapasowych tak, aby w momencie przejścia na wdrożone oprogramowanie do wykonywania backup-u dostępne były wszystkie kopie zapasowe zgodnie z ustawieniami retencji i protekcji,
- 5) Zmigruje taśmki LTO tak, aby w momencie przejścia na wdrożone oprogramowanie do wykonywania backup-u dostępne były wszystkie kopie zapasowe zgodnie z ustawieniami retencji i protekcji,
- 6) Skonfiguruje (zmigruje) zadania backupowe zgodnie z obecnie obowiązującymi ustawieniami 1:1.
- 7) Wykona testy akceptacyjne niezawodnościowe oraz funkcjonalne w tym:
 - backup na repozytorium i taśmy LTO vm, klastra SQL, serwerów AD; klastra Exchange.
 - odtworzenia vm z repozytorium i taśm LTO,
 - odtwarzania elementów AD z repozytorium,
 - odtworzenie elementów baz SQL,
 - odtwarzania elementów Exchange,
 - odtworzenie klastra SQL z taśm LTO.Odtworzenie z repozytorium i taśm LTO wymagane jest dla elementów zmigrowanych (vm, klaster SQL, konta AD, bazy SQL, klaster SQL, klaster Exchange, elementy poczty) z obecnie używanego oprogramowania Veeam, jak i z bieżących kopii bezpieczeństwa wykonanych w czasie wdrożenia.

Testy muszą się odbyć przed dostarczeniem **Dokumentacji powykonawczej**
- 8) Opracuje Dokumentację powykonawczą zawierającą opis wdrożonej konfiguracji (konfigurację poszczególnych serwerów, modułów, komponentów i usług) oraz procedury administracyjne i eksploatacyjne (w tym procedury awaryjnego odtwarzania funkcjonalności systemu, procedury bieżącego monitoringu oraz utrzymania i aktualizacji systemu) w zakresie uzgodnionym z Zamawiającym.
- 9) Dokumentacja powykonawcza wdrożonego oprogramowania do backupu, zostanie przekazana Zamawiającemu najpóźniej na 5 dni przed podpisaniem Protokołu odbioru Zadania II, w formie papierowej oraz w formie elektronicznej na pendrive w postaci plików do edycji i PDF.

1.2 Wymagania podstawowe:

- 1) Oprogramowanie musi być licencjonowanie w modelu "per-CPU". Wszystkie wymienione poniżej funkcjonalności muszą być zapewnione w tej licencji. Jakiegokolwiek dodatkowe licencjonowanie (per zabezpieczony TB, per vm, dodatkowo płatny backup agentowy dla środowiska wirtualizacyjnego objętego licencjonowaniem, dodatkowo płatna deduplikacja) nie jest dozwolone.
- 2) Oprogramowanie musi współpracować z infrastrukturą wirtualizacyjną VMware w wersjach 6.x, 7.x i 8.x oraz Microsoft Hyper-V 2012 R2, 2016, 2019 i 2022. Wszystkie funkcjonalności opisane w tej specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
- 3) Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- 4) Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
- 5) Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych, wspieranych przez vSphere i Hyper-V.
- 6) Ważność licencji nie może być ograniczona czasowo (licencje bezterminowe).
- 7) Oprogramowanie musi umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
- 8) Oprogramowanie musi tworzyć "samowystarczalne" archiwa, do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
- 9) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
- 10) Oprogramowanie 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 w takiej puli.

- 11) 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.
- 12) Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
- 13) Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie.
- 14) Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.
- 15) Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time).
- 16) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
- 17) Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
- 18) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
- 19) Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji.
- 20) Oprogramowanie musi oferować zarządzanie kluczami szyfrowania w przypadku utraty podstawowego klucza.
- 21) Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
- 22) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
- 23) Szyfrowanie ruchu - wymagane jest stosowanie protokołu TLS w wersji co najmniej 1.2.

1.3 Wymagania dotyczące wykonywania kopii zapasowych

- 1) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
- 2) 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.
- 3) Oprogramowanie musi oferować powyższy mechanizm z dokładnością do datastore'u.
- 4) Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
- 5) Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
- 6) Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
- 7) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
- 8) Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn do zdalnej lokalizacji z wykorzystaniem wbudowanej akceleracji WAN.
- 9) Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
- 10) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
- 11) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

- 12) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
- 13) Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z poziomu klienta webowego vSphere.
- 14) Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).

1.4 Wymagania dotyczące odtwarzania danych i systemów z kopii zapasowych.

- 1) Oprogramowanie musi umożliwić 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 niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania.
- 2) 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.
- 3) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
- 4) Oprogramowanie musi umożliwić odtworzenie plików na dowolną maszynę lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
- 5) Oprogramowanie musi mieć możliwość odtworzenia plików przy pomocy VMware VIX API
- 6) Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
 - i. Linux
 - ext3, ext4, JFS, XFS, Btrfs,
 - ii. BSD
 - UFS, UFS2
 - iii. Solaris
 - UFS, ZFS
 - iv. Windows
 - NTFS, FAT, FAT32, ReFS
- 7) Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Space.
- 8) Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- 9) Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
- 10) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2016 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- 11) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2012 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.
- 12) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
- 13) Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzania point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux bez konieczności pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
- 14) Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
- 15) Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows.

- 16) Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.

2. Produkt równoważny dla posiadanego pakietu Veeam Management Pack for System Center Operation Manager

2.1 W ramach prac wdrożeniowych Wykonawca:

- 1) Przygotuje szczegółowy **Projekt techniczny** realizacji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczanego oprogramowania oraz zawierający opis konfiguracji środowiska.
- 2) Wykona instalację i konfigurację wszystkich elementów oprogramowania wymaganych przez Zamawiającego.
- 3) Skonfiguruje infrastrukturę do monitoringu i uruchomi tak aby była w pełni funkcjonalna, zgodnie z Projektem technicznym.
- 4) Wykona testy akceptacyjne niezawodnościowe oraz funkcjonalne w tym mają wykazać spełnienie wymagań Zamawiającego odnośnie monitoring środowiska wirtualizacyjnego.
 - a. Testy muszą się odbyć przed dostarczeniem **Dokumentacji powykonawczej**
- 5) Opracuje **Dokumentację powykonawczą** zawierającą opis wdrożonej konfiguracji (konfigurację poszczególnych serwerów, modułów, komponentów i usług) oraz procedury administracyjne i eksploatacyjne (w tym procedury awaryjnego odtwarzania funkcjonalności systemu, procedury bieżącego monitoringu oraz utrzymania i aktualizacji systemu) w zakresie uzgodnionym z Zamawiającym.
- 6) Dokumentacja powykonawcza wdrożonego wdrożonego pakietu, zostanie przekazana Zamawiającemu najpóźniej na 5 dni przed podpisaniem Protokołu odbioru Zadania II, w formie papierowej oraz w formie elektronicznej na pendrive w postaci plików do edycji i PDF.

2.2 Wymagania podstawowe

- 1) Oprogramowanie musi być licencjonowanie w modelu "per-CPU".
- 2) Ważność licencji nie może być ograniczona czasowo (licencje bezterminowe).
- 3) Management Pack musi być zgodny i całkowicie integrować się z Microsoft System Center Operations Manager.
- 4) Management Pack musi zapewnić monitorowanie przez Microsoft System Center Operations Manager środowiska opartego o VMware ESXi 5.x, 6.x, 7.x i 8.x zarówno w wersji płatnej jak i pojedynczych hostów pracujących w oparciu o edycję darmową.
- 5) Management Pack musi zapewnić monitorowanie przez Microsoft System Center Operations Manager środowiska opartego o Windows Server Hyper-V 2012 R2, 2016, 2019,
- 6) Management Pack musi korzystać z wbudowanych w infrastrukturę VMware mechanizmów monitorowania (VMware API) i nie może instalować na infrastrukturze żadnych agentów.
- 7) Dla środowiska Hyper-V Management Pack musi móc się zintegrować i skorzystać z agentów Microsoft System Center Operations Managera.
- 8) Management Pack musi zapewnić możliwość monitorowania i raportowania o problemach wszystkich elementów infrastruktury VMware takich jak vCenter Server, klastry, hosty, wirtualne maszyny, wirtualne switchy, podsystemy dyskowe, hardware.
- 9) Management Pack musi zapewnić możliwość monitorowania i raportowania o problemach wszystkich elementów infrastruktury Hyper-V takich jak System Center Virtual Machine Manager, klastry, hosty, wirtualne maszyny, wirtualne switchy, podsystemy dyskowe.
- 10) Dane przesyłane podczas monitoringu muszą być zaszyfrowane i przesyłane przy pomocy protokołu HTTPS.
- 11) Management Pack musi mieć możliwość integracji z Microsoft System Center Virtual Machine Manager.
- 12) Management Pack musi zapewniać możliwość monitorowania i raportowania szczegółowych parametrów infrastruktury Veeam Backup&Replication.

III. Warunki gwarancji dla systemu backupu ujętego w zadaniu II

1. Zamawiający wymaga, aby dostarczone oprogramowanie, w ramach ceny za przedmiot zamówienia, były objęte opieką gwarancyjną przez cały okres wykupionego wsparcia producenta.
2. W ramach gwarancji Wykonawca zapewni:
 - a. usuwanie wad konfiguracyjnych oprogramowania;
 - b. przywracanie pełnej funkcjonalności działania komponentów systemu, w przypadku awarii;
 - c. aktualizacje systemu.
3. Wykonawca zapewni, w okresie trwania umowy, 100 bezpłatnych godzin asysty technicznej, w ramach której świadczyć będzie następujące usługi, w przypadku ich wystąpienia:
 - a. konsultacje w zakresie konfiguracji i eksploatacji systemu;
 - b. pomoc w rozwiązywaniu problemów technicznych związanych z funkcjonowaniem powstałego systemu;
 - c. rozbudowę lub modyfikację systemu.
4. Usługi asysty technicznej oraz opieki gwarancyjnej, zlecane będą, w miarę potrzeb Zamawiającego, drogą elektroniczną na adres poczty elektronicznej wskazany przez Wykonawcę.
5. Wykorzystanie liczby godzin asysty technicznej będzie dokumentowane, sporządzanym raz na 12 miesięcy, Protokołem odbioru asysty technicznej.
6. W przypadku konieczności zmiany Dokumentacji powykonawczej, w wyniku dokonania istotnych zmian konfiguracyjnych, Wykonawca zobowiązany jest dostarczyć zaktualizowaną dokumentację w terminie 30 dni roboczych po ich wykonaniu.
7. Wykonawca zobowiązuje się do świadczenia gwarancji i asysty technicznej na następujących zasadach:

Problem	Czas reakcji (godziny)	Czas przywrócenia systemu lub rozwiązanie zastępcze (godziny)	Czas naprawy - rozwiązania problemu (godziny)
Awaria krytyczna	4	24	48
Błąd	16	-	96

8. Problemy objęte gwarancją będą klasyfikowane, jako Awarie krytyczne i Błędy w następujący sposób:
 - a. awaria krytyczna: to sytuacja, w której brak jest możliwości użytkowania, co najmniej jednego z elementów Systemu.
 - b. błąd: sytuacja, której skutkiem jest brak możliwości użytkowania komponentu lub funkcjonalności Systemu.
 - c. czas reakcji rozumiany, jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem problemu do Serwisu Wykonawcy a czasem rozpoczęcia działań zmierzających do naprawy (wyeliminowania) zgłoszonego problemu.
 - d. czas przywrócenia systemu lub rozwiązania zastępczego problemu – czas liczony od momentu zgłoszenia, po którym rozwiązanie problemu, które może być realizowane poprzez zmianę parametrów Systemu, rekomendację modyfikacji procesu przetwarzania danych, rekomendację modyfikacji sprzętowo-programowej, rekomendację modyfikacji infrastruktury wykorzystywanej przez System lub inne rekomendacje prowadzące do zmiany kategorii problemu na niższą bądź do zamknięcia problemu – naprawy (rozwiązanie końcowe).
 - e. czas naprawy - rozwiązania problemu – maksymalny czas, po którym musi zostać przywrócona pełna funkcjonalność systemu, liczony od momentu zgłoszenia.
 - f. zastosowanie rozwiązania zastępczego nie zwalnia Wykonawcy z obowiązku dostarczenia dla niego właściwego rozwiązania końcowego.

9. Jeśli błąd dotyczy oprogramowania i Wykonawca uzyska diagnozę problemu wskazującą, że naprawa wymaga instalacji nowej wersji oprogramowania, Wykonawca zobowiązany jest przekazać Zamawiającemu treść diagnozy i zastosować rozwiązanie zastępcze problemu.
10. Na czas naprawy oprogramowania zostanie wstrzymany upływ czasu naprawy do czasu zainstalowania przez Wykonawcę nowej wersji oprogramowania wskazanej przez producenta oprogramowania.
11. Serwis w ramach udzielonej gwarancji, świadczony będzie w języku polskim zdalnie poprzez środki komunikacji elektronicznej lub w siedzibie Zamawiającego.
12. Zgłaszanie problemów będzie możliwe przez 7 dni tygodnia w godzinach 00:00-24:00 w sposób uzgodniony z Wykonawcą.
13. Zamawiający wymaga udostępnienia przez Wykonawcę Zamawiającemu, na jego prośbę, dostępu do informacji o zgłoszeniach.
14. Wykonawca przyjmie zgłoszenie i potwierdzi jego przyjęcie nie później niż do chwili upływu Czasu Reakcji, który wlicza się do Czasu rozwiązania problemu.
15. W razie wątpliwości uznaje się, że zgłoszenie zostało dokonane w chwili wystąpienia informacji w formie mailowej lub za pomocą dedykowanego narzędzia. Ryzyko nieotrzymania prawidłowo przekazanego zgłoszenia spoczywa na Wykonawcy, z wyjątkiem sytuacji, gdy Wykonawca udowodni, że nie otrzymał wiadomości z przyczyn od niego niezależnych.
16. Wskazane powyżej czasy liczone są od chwili dokonania zgłoszenia w sposób ciągły w odniesieniu do pojedynczego zgłoszonego problemu: Awarii lub Błędu.
17. Wszelkie koszty związane z naprawami, usuwaniem problemu, usług i transportu z i do siedziby Zamawiającego ponosi Wykonawca.
18. W przypadku stwierdzenia niezgodności w sposobie realizacji przez Wykonawcę zobowiązań gwarancyjnych, Zamawiający zastrzega sobie prawo do naliczenia kar umownych i potrącenia ich z Zabezpieczenia należytego wykonania umowy.
19. W przypadku, jeżeli Wykonawca nie wywiązuje się ze zobowiązań wynikających z gwarancji, Zamawiający może dokonać naprawy konfiguracji we własnym zakresie lub zlecić jej wykonanie osobie trzeciej, a kosztami obciążyć Wykonawcę z wykorzystaniem kwoty zabezpieczenia należytego wykonania umowy.
20. Zamawiający ma prawo dokonywania modyfikacji konfiguracji przez przeszkolonych pracowników, zgodnie z dokumentacją powykonawczą.
21. Wykonawca w okresie gwarancji jest zobowiązany co najmniej raz w roku od odbioru przedmiotu zamówienia, do wykonania wspólnie z Zamawiającym:
 - a. bezpłatnego przeglądu Systemu,
 - b. aktualizacji wymaganych lub rekomendowanych przez producenta lub producentów komponentów Systemu,
 - c. uruchomienia nowych, dostępnych w ramach aktualizacji funkcjonalności istotnych dla bezpieczeństwa teleinformatycznego.
22. W okresie gwarancji Wykonawca zapewni bezpłatnie dostarczanie nowych wersji oprogramowania oraz publikowanych poprawek wraz z ich instalacją.
23. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do stałego monitorowania podatności i luk bezpieczeństwa w systemie, w tym zobowiązuje się do prowadzenia okresowych lub na uzasadnione zlecenie Zamawiającego testów bezpieczeństwa i dostarczenia Zamawiającemu na jego żądanie, w terminie 2 dni od wykonania testu, raportów zawierających:
 - a. czynności wykonane w ramach testów,
 - b. wykryte podatności wraz z określeniem ich poziomu istotności oraz wskazaniem jakie zagrożenie powodują
 - c. wnioski oraz zalecenia dotyczące sugerowanych działań
 - d. wdrożone poprawki.
24. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do współpracy z Zamawiającym w zakresie wykrytych przez Zamawiającego bądź podmiot trzeci podatności i luk w systemie oraz zobowiązuje się do niezwłocznego wprowadzania zmian i poprawek w systemie, które wynikają

będą z rekomendacji po wykonanym teście, przy uwzględnieniu racjonalnych możliwości implementacji rekomendacji oraz przy uwzględnieniu, że ich wdrożenie nie naruszy praw autorskich do dostarczonego oprogramowania.

25. W okresie udzielonej gwarancji Wykonawca będzie współpracował z Zamawiającym w zakresie analizy raportów i testów bezpieczeństwa lub audytów systemów teleinformatycznych wykonanych niezależnie od przedmiotu umowy oraz wspierał obsługę i wprowadzanie koniecznych zmian i poprawek w Systemie wynikających z rekomendacji i możliwości implementacji, w zakresie w jakim nie narusza to praw autorskich do oprogramowania dostarczonego w ramach tego zamówienia.
26. Niezależnie od udzielonej gwarancji Zamawiającemu przysługuje rękojmia w zakresie przedmiotu zamówienia.

IV. Odbiór dostawy Zadania II

Potwierdzeniem odbioru dostawy wsparcia producenta oprogramowania będą podpisane z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego protokoły dostawy wsparcia producenta na min. pierwszy rok (informacja o terminie wsparcia musi być widoczna na stronie producenta oprogramowania i w konsoli oprogramowania Veeam po podmianie plików licencyjnych).

Rozdział IV

Zadanie III – Dostawa subskrypcji oprogramowania do wirtualizacji

I. Realizacja Zadania

Przedmiotem zadania jest dostawa subskrypcji oprogramowania do budowy systemu wirtualizacji umożliwiającego wirtualizację serwerów, zasobów dyskowych i sieci wraz z aktualizacją oprogramowania we wskazanej przez Zamawiającego infrastrukturze.

Obecnie Zamawiający wykorzystuje oprogramowanie VMware VCF 5.1 działające w oparciu o 4 klastry vCenter 8.0.2, dla których wsparcie producenta wygasa:

1. 4 serwery CPU 2x20 rdzeni 23,3 TiB vSan,
2. 5 serwerów CPU 2x20 rdzeni 296,9 TiB vSan,
3. 14 serwerów CPU 2x20 rdzeni 244,6 TiB vSan,
4. 7 serwerów CPU 2x8 rdzeni 448,4 TiB vSan.

Dodatkowo Zamawiający posiada składającą się z 6 serwerów infrastrukturę wchodzącą w skład dwóch klastrów vCenter VMware VCF, dla których wsparcie **wygasa w dniu 05.11.2025:**

1. 4 serwery CPU 2x20 rdzeni 69,8 TiB vSan,
2. 2 serwery CPU 2x8 rdzeni 128 TiB vSan.

Wymaganymi elementami zamówienia są:

1. Pakiet VMware Cloud Foundation lub oprogramowanie równoważne.
2. Oprogramowanie VMware vCenter Server lub oprogramowanie równoważne.
3. Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego. Za oprogramowanie równoważne do wskazanego w specyfikacji przy pomocy nazwy oraz źródła pochodzenia uznaje się oprogramowanie posiadające następujące cechy:
 - a) zakres funkcjonalny oprogramowania jest w pełni zgodny z zakresem funkcjonalnym oprogramowania wskazanego,
 - b) warunki licencjonowania oprogramowania nie mniej korzystne niż licencje oprogramowania wskazanego.
4. Wykazanie równoważności złożonej oferty leży po stronie Wykonawcy i w razie wątpliwości powinno zostać udokumentowane w możliwie najbardziej obiektywny sposób.

5. **3-letni okres wsparcia producenta** zapewniający dostęp do technicznej pomocy producenta oraz możliwość pobierania nowych wersji oprogramowania i poprawek, które powstaną w tym okresie, rozliczanego rocznie **dla 30 sztuk** serwerów fizycznych, dla których wsparcie producenta wygasa.
6. **Okres wsparcia producenta od dnia 06.11.2025** jeśli umowa zostanie podpisana w terminie wcześniejszym od daty zakończenia posiadanego wsparcia **do dnia zakończenia 3-letniego wsparcia dla 30 sztuk serwerów w celu zrównania daty zakończenia wsparcia dla wszystkich subskrypcji**, zapewniający dostęp do technicznej pomocy producenta oraz możliwość pobierania nowych wersji i poprawek, które powstaną w tym okresie, rozliczanego rocznie **dla 6 sztuk** serwerów fizycznych, dla których wsparcie wygasa **w dniu 05.11.2025**.
7. Ze względu na spójność środowiska i zapewnienie niezawodności platformy wirtualizacyjnej oraz uniknięcie zagrożeń mogących powstać na styku produktów różnych producentów całe oprogramowanie wirtualizacyjne musi być kompatybilne i ściśle ze sobą współpracować.
8. Dostarczane oprogramowanie musi być kompatybilne i ściśle współpracować z posiadaną przez Zamawiającego platformą sprzętową HPE Synergy 12000.
9. Dostarczane oprogramowanie musi być kompatybilne i ściśle współpracować z dostarczonym w ramach **Zadania II** oprogramowaniem do wykonywania kopii zapasowych.
10. Licencjonowanie musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta oprogramowania uaktualnień, poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania.
11. W ramach umowy Wykonawca ma zapewnić udzielanie uprawnień na witrynie producenta oprogramowania wskazanym przez Zamawiającego osobom (pracownikom Zamawiającego) do pobierania kodu zamówionego oprogramowania i kluczy licencyjnych.
12. Dostarczone oprogramowanie musi być w wersji najnowszej na dzień złożenia oferty.
13. System musi pracować w środowisku on-premise.
14. Dostarczone oprogramowanie nie może być zabronione do stosowania przez administrację któregośkolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).

II. Rozwiązania równoważne

1. Warunki równoważności dla elementów pakietu VMware Cloud Foundation oraz VMware vCenter Server w zakresie wirtualizacji serwerów i zarządzania środowiskiem serwerów wirtualnych są następujące:

- 1) Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM.
- 2) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
- 3) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
- 4) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
- 5) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo i 3 porty równoległe.
- 6) Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016 oraz następujące dystrybucje systemów Linux: Ubuntu 20.04, Debian 10 i Red Hat Enterprise Linux 8.
- 7) Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
- 8) Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych.
- 9) Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.

- 10) Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
- 11) Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- 12) Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
- 13) Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
- 14) Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
- 15) Oprogramowanie do wirtualizacji musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.
- 16) Oprogramowanie do wirtualizacji musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
- 17) Oprogramowanie do wirtualizacji musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) 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.
- 18) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia sieciowego w razie awarii karty sieciowej.
- 19) Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
- 20) Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE, w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
- 21) Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
- 22) Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.
- 23) Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
- 24) Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switch'y) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług.
- 25) Rozwiązanie musi posiadać natywne mechanizmy szyfrowania podczas przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
- 26) Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
- 27) Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych.
- 28) Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.

- 29) Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa, jak i zmianę jej wersji bez potrzeby wyłączenia wirtualnych maszyn.
- 30) 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.
- 31) Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu, po jakim taka decyzja jest wykonywana.
- 32) Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
- 33) Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
- 34) Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
- 35) Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
- 36) Rozwiązanie musi umożliwiać konfigurację wysokiej dostępności (HA) dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.
- 37) Oprogramowanie do wirtualizacji musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card.
- 38) Wirtualizator musi wspierać TPM 2.0. Oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, rozwiązanie gwarantuje, że wirtualizator uruchomił się w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego.
- 39) Wirtualizator musi mieć możliwość włączenia funkcji "Microsoft virtualization-based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows.
- 40) Rozwiązanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.
- 41) Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza to, że jeśli serwer fizyczny posiada funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizator na podstawie tych danych jest w stanie proaktywnie przenieść wszystkie maszyny wirtualne na inne, prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego.
- 42) Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/RAM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
- 43) Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
- 44) Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.
- 45) Przełącznik rozproszony musi współpracować z protokołem NetFlow.

- 46) Platforma wirtualizacji powinna w ramach przełącznika sieciowego zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.
- 47) Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.
- 48) Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii, a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.
- 49) Rozwiązanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju, na poziomie konkretnych maszyn wirtualnych.
- 50) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. procesorów, pamięci RAM, przestrzeni na dyskach/wolumenach).
- 51) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych.
- 52) Rozwiązanie powinno posiadać proaktywnie działający mechanizm, który przemigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii.
- 53) Rozwiązanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
- 54) Rozwiązanie musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.
- 55) Rozwiązanie musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.
- 56) Rozwiązanie jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy.
- 57) Rozwiązanie musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervisor i OS wirtualnej maszyny na wypadek sfalszowania lub podmiany).
- 58) Rozwiązanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU do maszyn wirtualnych.
- 59) Wirtualizator musi wspierać tzw. rozwiązanie trwałej, nieulotnej pamięci (Persistent Memory) zbliżonej do szybkości pamięci DRAM. W ten sposób wirtualizator może udostępnić dla maszyn wirtualnych dyski, które wspierają taką funkcjonalność - ultraszybką pamięć masową zbliżoną do pamięci DRAM.
- 60) Wirtualizator musi wspierać protokół Remote Direct memory Access (RDMA).
- 61) Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci). Centralna konsola graficzna powinna działać jako gotowa, wstępnie skonfigurowana maszyna wirtualna (tzw. virtual appliance).
- 62) Dostęp do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

- 63) Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
- 64) Rozwiązanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo musi być możliwość ustawienia harmonogramu wykonywania kopii zapasowej.

2. Warunki równoważności w zakresie wirtualizacji zasobów dyskowych:

- 1) Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD.
- 2) Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji odczytu/zapisu (Read/Write IO) po stronie serwerów fizycznych.
- 3) Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akceleryjacej operacji Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności "w locie".
- 4) Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania/dodatkowych maszyn wirtualnych.
- 5) Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną.
- 6) Rozwiązanie musi zapewniać możliwość budowy wspólnej wysokowydajnej i wysokodostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez minimalnie 3 serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 64 serwerów fizycznych.
- 7) Rozwiązanie musi zapewniać obsługiwane dysków wirtualnych maszyn do rozmiaru min. 62 TB.
- 8) Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniania przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak serwer fizyczny i jego komponenty takie jak dysk cache’ujący, dysk pojemnościowy.
- 9) Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
- 10) Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi centami przetwarzania danych, między różnymi szafami rack/chassis.
- 11) Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną stronę producenta, na której znajduje się lista wspieranych lub rekomendowanych konfiguracji. Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawcę/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery).
- 12) Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej.

- 13) Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.
- 14) Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych.
- 15) Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych.
- 16) W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) posiadający wbudowane mechanizmy typu Multi-Processor Fault Tolerance.
- 17) W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) pracujący niezależnie od systemów operacyjnych jakie wspiera.
- 18) Rozwiązanie musi posiadać na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 4 niezależnych producentów sprzętu serwerowego dostępnego na rynku Unii Europejskiej.
- 19) Oprogramowanie musi zapewniać natywną integrację (bez skryptów i/lub pluginów) z obecnie używanym przez Zamawiającego systemem zarządzania wirtualnym środowiskiem VMware Vcenter.
- 20) Rozwiązanie musi zapewniać możliwość zmniejszania przestrzeni dyskowej (odjęcie pojedynczego dysku, odjęcie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.
- 21) Rozwiązanie musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością w locie.
- 22) Rozwiązanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania/modyfikacji konfiguracji systemu.
- 23) Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej oraz musi umożliwiać wykorzystanie ww. przestrzeni dyskowej przez serwery fizyczne nie posiadające dysków wewnętrznych.
- 24) Rozwiązanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych do maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning.
- 25) Rozwiązanie musi mieć możliwość skonfigurowania deduplikacji i kompresji przy zapisie danych na dysk/grupę pojemnościową (składowanie danych).
- 26) Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla technologii deduplikacji oraz technologii implementującej RAID5 i RAID6 za pomocą oprogramowania.
- 27) Rozwiązanie musi umożliwiać szyfrowanie wirtualnych maszyn zlokalizowanych w zbudowanym w oparciu o rozwiązanie zasobie dyskowym oraz musi umożliwiać szyfrowanie maszyny wirtualnej bez przerywania jej pracy podczas przenoszenia na inny host lub zasób dyskowy.

3. Warunki równoważności w zakresie wirtualizacji sieci:

- 1) Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne.
- 2) Oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci protokołów sieciowych.
- 3) Rozwiązanie realizujące usługi wirtualnych sieci musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub plugin'ów nie wspieranych przez dostawcę platformy wirtualizatora serwerów.
- 4) Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego przełącznika instalowanego w jądrze wirtualizatora serwerów (Hypervisor), umożliwiającą tworzenie logicznych segmentów sieci

- L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta wirtualizatora serwerów.
- 5) Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego routera instalowanego w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników.
 - 6) Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN.
 - 7) Oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN oraz niezvirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów.
 - 8) Oprogramowanie musi zapewnić funkcjonalność wirtualnego routera wspierającego protokoły OSPF i BGP. Routing statyczny oraz BGP musi być możliwy poprzez tunel GRE.
 - 9) Rozwiązanie musi posiadać funkcję łączenia (bridge) segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie wirtualnej bramy (bridge).
 - 10) Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT).
 - 11) Rozwiązanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego.
 - 12) Oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API.
 - 13) Zmiana konfiguracji sieciowej musi odbywać się poprzez narzędzia zarządzające dostępne dla środowiska wirtualizacyjnego serwerów.
 - 14) Oprogramowanie powinno zapewniać wsparcie dla wykorzystania plików danych JSON oraz XML.
 - 15) Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do rozwiązań firm trzecich z obszaru bezpieczeństwa.
 - 16) Oferowane oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu – tj. load balancing działającą w warstwach 4 i 7 modelu ISO OSI dla protokołów TCP, UDP, SSL/TLS, HTTP/2.
 - 17) Funkcja Wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci.
 - 18) Rozwiązanie ma umożliwić użytkowanie **2 instancji, 2-rdzeniowego loadbalancera**.
 - 19) Rozwiązanie musi posiadać funkcję łączenia (bridge) segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika firm trzecich.
 - 20) Rozwiązanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) opartych o wirtualizację VMware vSphere.
 - 21) Rozwiązanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego oraz fizycznego.
 - 22) Rozwiązanie musi mieć możliwość wykorzystania wbudowanego kolektora w celach dalszej analizy ruchu.
 - 23) Rozwiązanie musi mieć możliwość wizualizacji połączeń maszyn wirtualnych do zasobów dyskowych, połączenia do hosta i wyjścia na zewnątrz do sieci fizycznej.
 - 24) Rozwiązanie do analizy przepływów sieciowych musi posiadać funkcjonalność API.

III. Odbiór dostawy

Potwierdzeniem odbioru dostawy będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego protokół dostawy subskrypcji wraz ze wsparciem producenta na pierwszy rok.

IV. W ramach prac aktualizacyjnych/wdrożenia systemu Wykonawca w oparciu o dostarczone oprogramowanie wykona następujące prace:

1. Przygotuje szczegółowy **Projekt techniczny** realizacji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczanego oprogramowania zawierający:
 - a) projekt architektury systemu,
 - b) usługi realizowane przez system,
 - c) konfigurację komponentów,
 - d) nazewnictwo komponentów,
 - e) model administrowania,
 - f) konfigurację ustawień bezpieczeństwa,
 - g) wykonywanie kopii zapasowych i odtwarzanie środowiska,
 - h) monitorowanie systemu,
 - i) listę procedur administracyjnych,
 - j) koncepcję aktualizacji.
2. Opracuje i uzgodni szczegółowy harmonogram realizacji prac.
3. Zaktualizuje oprogramowanie do najnowszej kompatybilnej ze sprzętem wersji lub skonfiguruje infrastrukturę zwirtualizowaną i uruchomi tak aby była w pełni funkcjonalna we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania (w tym monitoringu).
4. Dokona migracji wszystkich niezbędnych elementów systemu **jeśli zajdzie taka konieczność** np. maszyn wirtualnych-700 sztuk.
5. Zapewni integrację z MS Active Directory.
6. Skonfiguruje integrację z wewnętrznym systemowym i centralnym zewnętrznym syslogiem.
7. Wykona testy akceptacyjne (niezawodnościowe oraz funkcjonalne) oraz opracuje i przedstawi Raport z testów.
8. Opracuje **Dokumentację powykonawczą** zawierającą:
 - a) Opis architektury zaimplementowanego rozwiązania.
 - b) Szczegółowy opis instalacji i konfiguracji wykorzystywanego oprogramowania, ze wskazaniem wybranych opcji i ustawionych wartości. Konfigurację poszczególnych modułów, komponentów i usług.
 - c) Zbiór zaimplementowanych polityk konfiguracyjnych dla poszczególnych modułów.
 - d) Politykę i procedury wykonywania i przechowywania kopii zapasowych oraz ich testowania i odtwarzania.
 - e) Szczegółowe procedury administracyjne i eksploatacyjne oraz awaryjnego odtwarzania funkcjonalności systemu opisujące krok po kroku niezbędne czynności umożliwiające Zamawiającemu samodzielne przywrócenie funkcjonalności systemu.
 - f) Procedury i instrukcje bieżącego monitoringu oraz utrzymania i aktualizacji systemu.
 - g) Instrukcje dla użytkowników/administratorów.
 - h) Inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z Zamawiającym.

V. Odbiór aktualizacji/wdrożenia

1. Dokumentacja powykonawcza systemu do wirtualizacji, zostanie przekazana Zamawiającemu najpóźniej w dniu podpisania Protokołu odbioru aktualizacji/wdrożenia, w formie papierowej oraz w formie elektronicznej na pendrive w postaci plików do edycji i PDF.
2. Potwierdzeniem odbioru będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, Protokół odbioru aktualizacji/wdrożenia.

VI. Warunki gwarancji

1. Zamawiający wymaga, aby wszystkie dostarczone komponenty systemu, w ramach ceny za przedmiot zamówienia, były objęte opieką gwarancyjną na okres 3 lat, którego bieg rozpocznie się od dnia aktywacji subkrypcji dla 30 serwerów fizycznych.
2. W ramach gwarancji na system wirtualizacji Wykonawca zapewni:

- a) usuwanie wad konfiguracyjnych systemu,
- b) przywracanie pełnej funkcjonalności działania komponentów systemu, jeżeli ich niewłaściwe działanie bądź awaria wynika z instalacji lub konfiguracji zrealizowanych podczas aktualizacji/wdrożenia,
- c) aktualizację systemu.
3. Wykonawca zapewni, w okresie trwania umowy, 300 bezpłatnych godzin asysty technicznej, w ramach której świadczyć będzie następujące usługi, w przypadku ich wystąpienia:
 - a) konsultacje w zakresie konfiguracji i eksploatacji systemu,
 - b) pomoc w rozwiązywaniu problemów technicznych związanych z funkcjonowaniem systemu,
 - c) rozbudowę lub modyfikację systemu.
4. Usługi asysty technicznej oraz opieki gwarancyjnej, zlecane będą, w miarę potrzeb Zamawiającego, drogą elektroniczną na adres poczty elektronicznej wskazany przez Wykonawcę.
5. Wykorzystanie liczby godzin asysty technicznej będzie dokumentowane, sporządzanym raz na 12 miesięcy, Protokołem odbioru asysty technicznej.
6. W przypadku konieczności zmiany Dokumentacji powykonawczej, w wyniku dokonania istotnych zmian konfiguracyjnych, Wykonawca zobowiązany jest dostarczyć zaktualizowaną dokumentację w terminie 30 dni roboczych po ich wykonaniu.
7. Wykonawca zobowiązuje się do świadczenia gwarancji i asysty technicznej na następujących zasadach:

Problem	Czas reakcji (godziny)	Czas przywrócenia systemu lub rozwiązanie zastępcze (godziny)	Czas naprawy - rozwiązania problemu (godziny)
Awaria krytyczna	2	12	48
Błąd	8	-	96

8. Problemy objęte gwarancją i asystą techniczną będą klasyfikowane, jako awarie krytyczne i błędy w następujący sposób:
 - a) awaria krytyczna: to sytuacja, w której brak jest możliwości użytkowania, co najmniej jednego z elementów systemu.
 - b) błąd: sytuacja, której skutkiem jest brak możliwości użytkowania komponentu lub funkcjonalności systemu.
 - c) czas reakcji rozumiany, jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem problemu do serwisu Wykonawcy a czasem rozpoczęcia działań zmierzających do naprawy (wyeliminowania) zgłoszonego problemu.
 - d) czas przywrócenia systemu lub rozwiązania zastępczego problemu – czas liczony od momentu zgłoszenia, po którym rozwiązanie problemu, które może być realizowane poprzez zmianę parametrów systemu, rekomendację modyfikacji procesu przetwarzania danych, rekomendację modyfikacji sprzętowo-programowej, rekomendację modyfikacji infrastruktury wykorzystywanej przez system lub inne rekomendacje prowadzące do zmiany kategorii problemu na niższą bądź do zamknięcia problemu – naprawy (rozwiązanie końcowe).
 - e) czas naprawy - rozwiązania problemu – maksymalny czas, po którym musi zostać przywrócona pełna funkcjonalność systemu, liczony od momentu zgłoszenia.
 - f) zastosowanie rozwiązania zastępczego nie zwalnia Wykonawcy z obowiązku dostarczenia dla niego właściwego rozwiązania końcowego.

9. Jeśli błąd dotyczy oprogramowania i Wykonawca uzyska diagnozę problemu wskazującą, że naprawa wymaga instalacji nowej wersji oprogramowania, Wykonawca zobowiązany jest przekazać Zamawiającemu treść diagnozy i zastosować rozwiązanie zastępcze problemu.
10. Na czas naprawy oprogramowania zostanie wstrzymany upływ czasu naprawy do czasu zainstalowania przez Wykonawcę nowej wersji oprogramowania wskazanej przez producenta oprogramowania.
11. Serwis w ramach udzielonej gwarancji, świadczony będzie w języku polskim zdalnie poprzez środki komunikacji elektronicznej lub w siedzibie Zamawiającego.
12. Zgłaszanie problemów będzie możliwe przez 7 dni tygodnia w godzinach 0:00-24:00 w sposób uzgodniony z Wykonawcą.
13. Zamawiający wymaga udostępnienia przez Wykonawcę Zamawiającemu, na jego prośbę, dostępu do informacji o zgłoszeniach.
14. Wykonawca przyjmie zgłoszenie i potwierdzi jego przyjęcie nie później niż do chwili upływu czasu reakcji, który wlicza się do czasu rozwiązania problemu.
15. W razie wątpliwości uznaje się, że zgłoszenie zostało dokonane w chwili wystąpienia informacji w formie mailowej lub za pomocą dedykowanego narzędzia. Ryzyko nieotrzymania prawidłowo przekazanego zgłoszenia spoczywa na Wykonawcy, z wyjątkiem sytuacji, gdy Wykonawca udowodni, że nie otrzymał wiadomości z przyczyn od niego niezależnych.
16. Wskazane powyżej czasy liczone są od chwili dokonania zgłoszenia w sposób ciągły w odniesieniu do pojedynczego zgłoszonego problemu: awarii lub błędu.
17. Wszelkie koszty związane z naprawami, usuwaniem problemu, usług i transportu z i do siedziby Zamawiającego ponosi Wykonawca.
18. W przypadku stwierdzenia niezgodności w sposobie realizacji przez Wykonawcę zobowiązań gwarancyjnych, Zamawiający zastrzega sobie prawo do naliczenia kar umownych i potrącenia ich z Zabezpieczenia należytego wykonania umowy.
19. W przypadku, jeżeli Wykonawca nie wywiązuje się ze zobowiązań wynikających z gwarancji, Zamawiający może dokonać naprawy konfiguracji we własnym zakresie lub zlecić jej wykonanie osobie trzeciej, a kosztami obciążyć Wykonawcę z wykorzystaniem kwoty zabezpieczenia należytego wykonania umowy.
20. Zamawiający ma prawo dokonywania modyfikacji konfiguracji przez przeszkolonych pracowników, zgodnie z dokumentacją powykonawczą.
21. Wykonawca w okresie gwarancji jest zobowiązany co najmniej raz w roku od odbioru przedmiotu zamówienia, do wykonania wspólnie z Zamawiającym:
 - a) corocznie bezpłatnego przeglądu systemu,
 - b) aktualizacji wymaganych lub rekomendowanych przez producenta lub producentów komponentów systemu,
 - c) uruchomienia nowych, dostępnych w ramach aktualizacji funkcjonalności istotnych dla bezpieczeństwa teleinformatycznego.
22. W okresie gwarancji Wykonawca zapewni bezpłatnie dostarczanie nowych wersji oprogramowania oraz publikowanych poprawek wraz z ich instalacją.
23. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do stałego monitorowania podatności i luk bezpieczeństwa w systemie, w tym zobowiązuje się do prowadzenia okresowych lub na uzasadnione zlecenie Zamawiającego testów bezpieczeństwa i dostarczenia Zamawiającemu na jego żądanie, w terminie 5 dni od wykonania testu, raportów zawierających:
 - a) czynności wykonane w ramach testów,
 - b) wykryte podatności wraz z określeniem ich poziomu istotności oraz wskazaniem jakie zagrożenie powodują,
 - c) wnioski oraz zalecenia dotyczące sugerowanych działań,
 - d) wdrożone poprawki.
24. W okresie udzielonej gwarancji Wykonawca zobowiązuje się do współpracy z Zamawiającym w zakresie wykrytych przez Zamawiającego bądź podmiot trzeci podatności i luk w systemie

oraz zobowiązuje się do niezwłocznego wprowadzania zmian i poprawek w systemie, które wynikać będą z rekomendacji po wykonanym teście, przy uwzględnieniu racjonalnych możliwości implementacji rekomendacji oraz przy uwzględnieniu, że ich wdrożenie nie naruszy praw autorskich do dostarczonego oprogramowania.

25. W okresie udzielonej gwarancji Wykonawca będzie współpracował z Zamawiającym w zakresie analizy raportów i testów bezpieczeństwa lub audytów systemów teleinformatycznych wykonanych niezależnie od przedmiotu umowy oraz wspierał obsługę i wprowadzanie koniecznych zmian i poprawek w Systemie wynikających z rekomendacji i możliwości implementacji, w zakresie w jakim nie narusza to praw autorskich do oprogramowania dostarczonego w ramach tego zamówienia.
26. Niezależnie od udzielonej gwarancji Zamawiającemu przysługuje rękojmia w zakresie przedmiotu zamówienia.

Opracowali

Zadanie I

Zadanie II

Zadanie III