Załącznik nr 2 do SWZ

Opis przedmiotu zamówienia

I. Przedmiot zamówienia:

Dostawa w modelu subskrypcji oprogramowania na okres od 25.11.2024 do 20.06.2027 r., zgodnie z poniższą tabelą:

Nazwa	P/N	Opis	Ilość
VSPHERE FOUNDATION	VCF-VSP-FND-8	VMware vSphere Foundation 8, SW Bundle, minimum 16 core per CPU	80 szt.
VSAN	VCF-VSAN-8	VMware vSAN 8, TiB	49 szt.

Zamawiający oczekuje zrównania okresu licencjonowania zamawianych nowych subskrypcji z posiadanymi już subskrypcjami tak, by okres zakończenia dla nowych subskrypcji kończył się z dniem posiadanych subskrypcji tj. w dniu **20.06.2027 r**.

II. Termin, dostawa potwierdzania przedłużenia usługi:

Dostawa licencji nastąpi nie wcześniej niż 18.11.2024 r. i nie później niż w dniu 25.11.2024 r.

Kryteria równoważności dla oprogramowania VMWARE:

Dostarczone rozwiązanie musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

1. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
2. 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.
3. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
7. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2016, Windows Server 2019, Windows 11, SLES 15 SLES 12, SLES 11, REHL 7, RHEL 6, RHEL 5, REHL Atomic 7, Solaris

11 ,Solaris 10, Solaris 9, Solaris 8, Debian, CentOS, FreeBSD, Mandriva, Ubuntu, Mac OS X, Oracle Linux.

8. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
9. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych.
10. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
11. 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.
12. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
13. 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.
14. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
15. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
16. Rozwiązanie 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.
17. 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.
18. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
19. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
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. Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut.
25. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług.
26. Rozwiązanie musi mieć możliwość oraz zapewniona musi być odpowiednia licencja umożliwiająca przenoszenie maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. System musi zapewnić możliwość równoważenia

obciążenia, automatycznie przenosząc maszyny wirtualne pomiędzy serwery. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi.
27. 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.
28. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych.
29. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
30. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn.
31. 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.
32. 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.
33. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
34. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
35. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
36. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
37. Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.
38. Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe).
39. System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.
40. 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, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego.
41. Wirtualizator musi mieć możliwość włączenia funkcji “Microsoft virtualization- based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 11 oraz Windows Server 2019.
42. System musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.

43. Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 11 oraz Windows 2019. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 11 lub Windows 2019 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora.
44. Wirtualizator musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego – następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji.
45. Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich posiadanych przez Zamawiającego serwerów (6 sztuk) wchodzących w skład klastra wysokiej dostępności.
46. Rozwiązanie musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji. System musi umożliwiać zarządzanie całą warstwą wirtualizacji z jednego bezpiecznego systemu do zarządzania z kontrolą dostępu.
47. 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.
48. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
49. Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
50. 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.
51. Przełącznik rozproszony musi współpracować z protokołem NetFlow.
52. Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.
53. Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu
sieciowego dowolnego jego portu wirtualnego na inny port.
54. 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.

55. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych.
56. System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.
57. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane z okresu co najmniej 12 ostatnich miesięcy.
58. 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 platformami wirtualnej.
59. 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.
60. Rozwiązanie musi posiadać proaktywnie działający mechanizm, który dokona migracji wirtualnych maszyn po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii.
61. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
62. System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.
63. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
64. System 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.
65. 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.
66. System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervizor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany).

W przypadku zastosowania rozwiązania równoważnego Oferent zapewni:

Zamawiający informuje, że na chwilę obecną posiada 6 jednakowych serwerów fizycznych, działających jako jeden klaster wysokiej dostępności. Sumaryczna ilość danych zajętych w klastrze wynosi około 40 TB. W klastrze pracuje 71 maszyn wirtualnych.

1. Oferent przedstawi harmonogram prac związanych z wdrożeniem i migracją systemów Zamawiającego w godzinach 8:00-16:00 od poniedziałku do piątku.
2. Oferent wdroży rozwiązanie równoważne w infrastrukturze Zamawiającego w terminie nie dłuższym niż 10 dni roboczych od daty podpisania umowy.
3. W ramach wdrożenia, Oferent wykona testy wdrożonego rozwiązania uwzględniające min.

a. utratę do dwóch serwerów zamawiającego jednocześnie (z sześciu posiadanych),
b. utratę zasilania dla wszystkich (sześciu) serwerów Zamawiającego,
c. migrację maszyn wirtualnych pomiędzy serwerami.

4. Na czas dostarczenia i wdrożenia rozwiązania równoważnego, Oferent zapewni:
   a. sprzęt i oprogramowanie
   b. personel techniczny

   z pomocą którego Oferent dokona w sposób bezprzerwowy dla pracy systemów Zamawiającego (SLA na poziomie 99,9%), migracji posiadanych przez Zamawiającego zasobów ze środowiska VMware do środowiska Oferenta a następnie po instalacji rozwiązania równoważnego w infrastrukturze Zamawiającego, dokona migracji ze środowiska Oferenta do środowiska Zamawiającego.
5. Oferent pokryje koszt energii elektrycznej niezbędnej do utrzymania dodatkowej infrastruktury na podstawie wskazań certyfikowanego podlicznika energii elektrycznej, który Oferent dostarczy na czas wdrożenia.
6. Autoryzowane szkolenie dla 6 administratorów Zamawiającego w formie vouchera na kurs podstawowej i kurs zaawansowanej obsługi oferowanego systemu do wykorzystania w ciągu 6-ciu miesięcy przez pracowników Zamawiającego.
7. W okresie 6 miesięcy od daty dostarczenia równoważnego rozwiązania Oferent zapewni wsparcie certyfikowanych specjalistów w zakresie niezbędnym do utrzymania infrastruktury Zamawiającego (bieżące utrzymanie infrastruktury, aktualizacje bezpieczeństwa, zgłoszenia awarii). Wsparcie dostępne 7 dni w tygodniu, z czasami reakcji:
   a. **Incydenty krytyczne** (np. awarie sprzętu, przestoje w pracy serwerów, brak dostępu do danych):
      Czas reakcji: 1 godzina.
      Rozpoczęcie naprawy: natychmiastowe po wykryciu.
      Rozwiązanie problemu: do 4 godzin.
   b. **Incydenty średniego poziomu** (np. ograniczona dostępność, drobne problemy z wydajnością):
      Czas reakcji: 2 godziny.
      Rozpoczęcie naprawy: do 4 godzin.
      Rozwiązanie problemu: do 24 godzin.
   c. **Incydenty niskiego poziomu** (np. żądania konfiguracji, zapytania o raporty):
      Czas reakcji: do 8 godzin.
      Rozwiązanie problemu: do 3 dni roboczych.
8. W celu szybkiego wykrywania problemów, bez konieczności zgłaszania ich przez Zamawiającego, na czas wdrożenia rozwiązania równoważnego oferent zapewni monitoring infrastruktury i systemów Zamawiającego w trybie 24/7.
9. Na czas wdrożenia rozwiązania równoważnego, Oferent zapewni wykonywanie kopii bezpieczeństwa wszystkich systemów Zamawiającego (minimum jedna kopia dziennie, poza godzinami pracy Biura tj. w godzinach 17:00-7:00).
