*4 Załącznik nr 1 do Zapytania Ofertowego*

**Szczegółowy Opis Przedmiotu Zamówienia (SOPZ)**

**„ Zakup Oprogramowania i świadczenie usług w zakresie dostosowania infrastruktury, Serwis Gwarancyjnego, Serwisu Pogwarancyjnego oraz wykonywanie Prac Zleconych w obszarze Chmury Prywatnej typu SDDC na potrzeby Ogólnopolskiej Sieci Edukacyjnej”**

**znak postępowania: xxxxxxxxx[OSE2025]**

# Spis treści

[Spis treści 2](#_Toc215846682)

[1. Definicje 4](#_Toc215846683)

[2. Chmura Prywatna 9](#_Toc215846684)

[2.1 Platforma Konteneryzacyjna w ramach Chmury Prywatnej 9](#_Toc215846685)

[3. Opis przedmiotu zamówienia 9](#_Toc215846686)

[3.1 Opis ogólny 9](#_Toc215846687)

[3.2 Opis Serwisu Gwarancyjnego 10](#_Toc215846688)

[3.3 Opis Serwisu Pogwarancyjnego 11](#_Toc215846689)

[3.4 Założenia techniczne 12](#_Toc215846690)

[3.5 Wymagania w zakresie architektury 15](#_Toc215846691)

[3.6 Skalowalność 15](#_Toc215846692)

[4. Zakres Umowy 15](#_Toc215846693)

[4.1 Oprogramowanie stosowane w Chmurze Prywatnej 16](#_Toc215846694)

[4.2 Serwery HCI stosowane w Chmurze Prywatnej 16](#_Toc215846695)

[4.3 Docelowa architektura Chmury Prywatnej 18](#_Toc215846696)

[4.4 Zamówienie podstawowe, pakiet Prac Zleconych 19](#_Toc215846697)

[4.5 Zamówienie Opcjonalne AS – rozszerzenie pakietu Prac Zleconych dla oprogramowania, 10 pakietów po 200 godzin 19](#_Toc215846698)

[4.6 Zamówienie Opcjonalne AH – rozszerzenie pakietu Prac Zleconych dla sprzętu, 5 pakietów po 100 godzin 20](#_Toc215846699)

[5. Docelowa architektura Chmury Prywatnej 20](#_Toc215846700)

[5.1 Architektura Chmury Prywatnej – etap A 20](#_Toc215846701)

[5.2 Architektura Chmury Prywatnej – etap B, kontynuacja zmian z etapu A 27](#_Toc215846702)

[5.3 Architektura Chmury Prywatnej – etap C 32](#_Toc215846703)

[5.4 Orkiestracja procesu DR pomiędzy OPD1 i OPD2 37](#_Toc215846704)

[Wymagania w zakresie funkcjonalności oprogramowania Chmury Prywatnej 38](#_Toc215846705)

[5.5 Wymagania w zakresie funkcjonalności monitorowania Chmury Prywatnej 38](#_Toc215846706)

[5.6 Wymagania w zakresie realizacji Umowy 38](#_Toc215846707)

[6. Wymogi na równoważność dla Oprogramowania SDDC 40](#_Toc215846708)

[7. Usługi w ramach Prac Zleconych 70](#_Toc215846709)

[7.1 Zakres Prac Zleconych: 70](#_Toc215846710)

[7.2 Zlecanie Prac Zleconych: 71](#_Toc215846711)

[7.3 Poziomy świadczenia usługi Prac Zleconych 72](#_Toc215846712)

[7.4 Realizacja Prac Zleconych 73](#_Toc215846713)

[7.5 Testy Odbiorcze dla Prac Zleconych 73](#_Toc215846714)

[7.6 Odbiór Prac Zleconych 73](#_Toc215846715)

[8. Usługi Serwisowe 74](#_Toc215846716)

[9. Serwis Pogwarancyjny 74](#_Toc215846717)

[9.1 Ogólne warunki Serwisu Pogwarancyjnego 75](#_Toc215846718)

[10. Serwis Gwarancyjny 77](#_Toc215846719)

[10.1 Ogólne warunki Serwisu Gwarancyjnego 77](#_Toc215846720)

[10.2 Opis usług Serwisu Gwarancyjnego 78](#_Toc215846721)

[10.3 Raportowanie usług Serwisu Gwarancyjnego 85](#_Toc215846722)

# Definicje

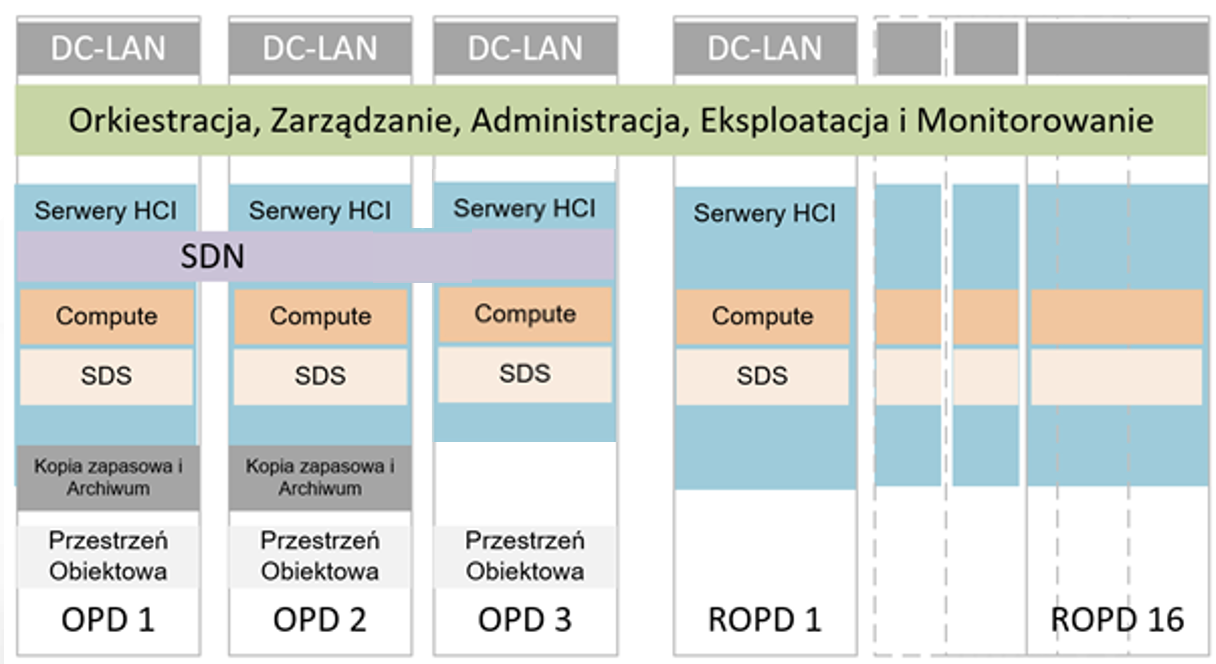
|  |  |
| --- | --- |
| Definicja | Opis |
| Advanced NG-Firewall | Zapora sieciowa nowej generacji to zaawansowane rozwiązanie bezpieczeństwa sieciowego, które łączy tradycyjne funkcje zapory ogniowej z dodatkowymi, możliwościami. Obejmuje ona inspekcję na poziomie aplikacji (w tym identyfikację aplikacji, niezależnie od portu);  systemy zapobiegania włamaniom (IPS - Intrusion Prevention System), który monitoruje i blokuje złośliwy ruch sieciowy w czasie rzeczywistym;  systemy rozpoznawania zagrożeń (IDS - Intrusion Detection System) wykrywania włamań, który monitoruje ruch sieciowy wykrywając podejrzane działania lub potencjalne zagrożenia, np. próby włamania,  Filtrowanie adresów URL (URL-Filtering) to technika, która blokuje lub zezwala na dostęp do określonych stron internetowych na podstawie predefiniowanych zasad umożliwiając dostęp wyłącznie do stron wskazanych lub blokowanie grupy stron zakazanych zgodnie z kategorią stron aktualizowaną z bazy zewnętrznej producenta;  ochrona zasobów obliczeniowych przed złośliwym oprogramowaniem (malware) składająca się na zestaw narzędzi zabezpieczających systemy komputerowe przed niechcianym i szkodliwym oprogramowaniem m.in. wirusami, trojanami i innymi zagrożeniami. |
| Aktualizacje Oprogramowania (Aktualizacje) | Dostarczone lub udostępnione przez Wykonawcę lub producenta Oprogramowania, w ramach realizacji przedmiotu zamówienia najnowsze komercyjnie dostępne wersje Oprogramowania oraz udoskonalenia wersji bieżących Oprogramowania. |
| Architekt | Specjalista z wieloletnim doświadczeniem odpowiedzialny za projektowanie, tworzenie i nadzorowanie wdrażania złożonych systemów informatycznych i infrastruktury w organizacji. Jego rolą jest zapewnienie, że rozwiązania technologiczne są zgodne z postawionymi celami a jednocześnie efektywne, skalowalne, bezpieczne i zgodne z założonymi normami. Architekt koordynuje prace zespołów technicznych, działa jako mediator między potrzebami biznesu a możliwościami technologicznymi. |
| Awaria Istotna | Wystąpienie Problemu, w wyniku którego zostaje spełniona jedna z przesłanek wymienionych w pkt 10 (Serwis Gwarancyjny) ppkt 10.2. |
| Awaria Krytyczna | Wystąpienie Problemu, w wyniku którego zostaje spełniona jedna z przesłanek wymienionych w pkt 10 (Serwis Gwarancyjny) ppkt 10.2. |
| Awaria Poważna | Wystąpienie Problemu, w wyniku którego zostaje spełniona jedna z przesłanek wymienionych w pkt 10 (Serwis Gwarancyjny) ppkt 10.2. |
| AZ-1  AZ-2  AZ-3 | Strefa dostępności stanowiąca niezależny obszar funkcjonalny w obszarze data center zapewniający operacyjną pracę usługi w przypadku awarii lub problemów z dostępnością jednego z obszarów.  AZ-1 odpowiada lokalizacji OPD-1  AZ-2 odpowiada lokalizacji OPD-2  AZ-3 odpowiada lokalizacji OPD-3 |
| Błędy i Wady | Każda niezgodność Oprogramowania i Urządzeń z wymaganiami Umowy i /lub niespełniające wymagań funkcjonalnych, pojemnościowych i/lub wpływające na zakres i jakość usług spełnianych przez Oprogramowanie lub Urządzenia, a także na wydajność Chmury Prywatnej, stwierdzona na etapie Testów Odbiorczych. |
| Chmura Prywatna | Rozwiązanie informatyczne stanowiące część Systemu, składające się z oprogramowania SDDC i urządzeń (serwerów). Kompleksowe rozwiązanie zapewniające wirtualizacje zasobów (Compute Storage i Network) celem udostępniania usług w modelu zapewniającym automatyzację procesu powoływania, utrzymania i usuwania poprzez wykorzystanie narzędzi SDDC upraszczających procesy operacyjno-administracyjne z monitorowaniem. Integralną częścią Chmury Prywatnej jest Platforma Kontenerowa uzupełniająca architekturę SDDC o obszar K8s (Cloud Native). |
| Czas Przywrócenia | Czas od Zgłoszenia Problemu do momentu zastosowania Obejścia niwelującego zgłoszony problem. |
| Czas Reakcji | Czas od Zgłoszenia Problemu do momentu potwierdzenia przez Wykonawcę do Zamawiającego przyjęcia Zgłoszenia Problemu. |
| Czas Rozwiązania Problemu | Czas od Zgłoszenia Problemu do momentu Rozwiązania Problemu, ustania przyczyny zgłoszonego problemu. |
| Dokumentacja | Dokumenty wytworzone w związku z realizacją przedmiotu zamówienia i bieżące aktualizacje dodawane wraz z rozwojem i modyfikacją. |
| Dokumentacja Powykonawcza | Zestaw rysunków, tekstów i innych dokumentów obrazujących stan infrastruktury wykonanej przez Wykonawcę w ramach Umowy w chwili Odbioru, wraz z późniejszymi aktualizacjami-modyfikacjami, o ile nastąpią zmiany w okresie umowy. |
| Dokumentacja Techniczna | Zbiór dokumentów wytworzonych przez Wykonawcę w ramach realizacji Umowy i podlegający akceptacji przez Zamawiającego. W skład Dokumentacji Technicznej wchodzi koncepcja rozwiązania (HLD) i projekt techniczny (LLD), wraz z rozwojem, modyfikacją i harmonogramem. |
| Dysk | Nośnik danych - pamięć masowa, która umożliwia zapis, przechowanie i przetwarzanie danych zapisanych, np. SSD, NVMe. |
| Dzień Roboczy | Każdy dzień tygodnia z wyjątkiem sobót, niedziel i innych dni ustawowo wolnych od pracy na terytorium RP. |
| ESXi | <https://knowledge.broadcom.com/external/article/316595/build-numbers-and-versions-of-vmware-esx.html>  jest to oprogramowanie producenta VMware/Broadcom stosowane do wirtualizacji zasobów obliczeniowych – hypervisor, wraz z rozwiązaniami SDS i SDN stanowiące architekturę SDDC stosowaną przez Zamawiającego. |
| HCI (Hyper-Converged Infrastructure) | Hiperkonwergentna łatwo skalowalna infrastruktura centrum danych budowana z powtarzalnych komponentów - serwery x86. Technologia dostarczająca zbiór zasobów: moc obliczeniową (procesory), współdzielony system pamięci masowej i rozwiązania sieciowe, przy zastosowaniu oprogramowania SDDC. |
| HLD (High-level design) | Dokumentacja opisująca planowaną architekturę i harmonogram implementacji projektu m.in. założenia do procesu wdrożenia i planowanej konfiguracji. |
| Komponenty | Bloki funkcjonalne składające się na System, tj.: Serwery, Macierz Deduplikator, Oprogramowanie SDDC. |
| Konsultacje | Element Serwisu Gwarancyjnego i Pogwarancyjnego świadczonego przez Wykonawcę, obejmujący zapewnienie dostępu do wykwalifikowanej „certyfikowanej” pomocy technicznej Wykonawcy jako wsparcia w rozwiązywaniu Problemów związanych z bieżącą eksploatacją Przedmiotu Umowy. Szczegółowy zakres Konsultacji określa pkt 8. |
| Koordynator zmiany | Menedżer zmian, odpowiedzialny za zarządzanie wszystkimi aspektami zmian. Ustala priorytet zmiany, wnioskuje o akceptacje, ocenia ich wpływ oraz akceptuje lub odrzuca zmiany. |
| LLD (Low-level design) | Szczegółowa Dokumentacja opisująca techniczne szczegóły implementacji projektu np. schematy i dane szczegółowe w zakresie konfiguracji i ustawienia m.in. Excel, YAML i inne pliki. |
| NVMe | Dysk półprzewodnikowy ([ang.](https://pl.wikipedia.org/wiki/J%C4%99zyk_angielski) Non-Volatile Memory Express) – pamięć masowa zbudowane w oparciu o [pamięć flash](https://pl.wikipedia.org/wiki/Pami%C4%99%C4%87_flash) zapewniając dostęp do pamięci trwałej poprzez magistralę PCI Express (PCIe). |
| Obejście | Tymczasowe Rozwiązanie Problemu. Obejście nie stanowi Rozwiązania Problemu, jednak pozwala korzystać z wszystkich funkcjonalności Systemu również, gdy wymaga to podejmowania dodatkowych czynności przez użytkowników. |
| Odbiór prac zleconych | Szereg czynności mających na celu potwierdzenie zrealizowanych prac. |
| Opcje | Określone zobowiązania lub zadania wykonywane przez Wykonawcę w okresie Umowy możliwe do zamówienia przez Zamawiającego w ramach przedmiotu umowy. |
| OPD | Istniejące w OSE Centralne Ośrodki Przetwarzania Danych, oznaczone odpowiednio:  OPD1 - WARSZAWA  OPD2 - POZNAŃ  OPD3 - KATOWICE |
| Operator OSE | Przedsiębiorca telekomunikacyjny świadczący usługi dostępu do Internetu za pośrednictwem OSE na rzecz szkół. Operator OSE odpowiada za podłączanie szkół, a następnie obsługuje je na bazie wewnętrznych i zewnętrznych struktur organizacyjnych, zawierających między innymi Centrum Kontaktu, Centrum Zarządzania Siecią oraz Centrum Zarządzania Bezpieczeństwem. |
| Oprogramowanie | Oprogramowanie, instalowane na sprzęcie Zamawiającego w ramach realizacji Umowy wraz z dokumentacją, modyfikacjami, uaktualnieniami, nowymi wersjami, spełniające wymagania opisane w SOPZ, które ma być dostarczone przez Wykonawcę na rzecz Zamawiającego w ramach realizacji przedmiotu zamówienia, o ile występuje w wymaganiach. |
| Plan Testów | Dokument definiujący zakres i sposób prowadzenia Testów Odbiorczych dla usług i zadań zleconych , opracowany zgodnie z wytycznymi zawartymi pkt 7, przygotowany przez Wykonawcę zgodnie z wymaganiami SOPZ i Zamawiającego, podlegający akceptacji Zamawiającego. |
| Platforma Kontenerowa/Platforma  (Cloud Native) | Kompleksowe rozwiązanie programowe tworzące wirtualną przestrzeń do udostępniania usług w modelu mikroserwisów stosującą DevOps poprzez budowę rozwiązania do tworzenia i zarządzania klastrami Kubernetes z narzędziami administracyjnymi i monitorowaniem. |
| Prace Zlecone | Zadania zlecone w ramach Chmury Prywatnej i Opcji, m.in. zadania rozwojowe, migracyjne, relokacyjne, konfiguracyjne, aktualizacyjne, projektowe i inne zlecone, opisane w niniejszym dokumencie. |
| Problem | Zdarzenie, które uniemożliwia lub w jakikolwiek sposób ogranicza możliwość korzystania przez Zamawiającego z Oprogramowania lub Urządzeń zgodnie z wymaganiami opisanymi w Umowie, Problemy będą kategoryzowane jako Awaria Istotna, Awaria Krytyczna, Awaria Poważna i Usterka. |
| Przywrócenie | Zastosowanie Obejścia. |
| ROPD | Istniejące w chmurze prywatnej Zamawiającego Regionalne Ośrodki Przetwarzania Danych, oznaczone odpowiednio:  ROPD1, ROPD2 – do ROPD16 są to lokalne centra obliczeniowe w węzłach sieci OSE. |
| Rozwiązanie Problemu | Ostateczne usunięcie Problemu przez Wykonawcę. |
| Serwis Gwarancyjny | Usługa świadczona na rzecz Zamawiającego obejmująca między innymi zobowiązania Wykonawcy do usuwania awarii i Problemów oraz innych czynności określonych w pkt 10 przy wsparciu producenta. |
| Serwis Pogwarancyjny | Usługa świadczona na rzecz Zamawiającego obejmująca zobowiązania Wykonawcy do diagnozowania zgłaszanych awarii i Problemów dotyczących oprogramowania VMware (HCI-KIT) dla lokalizacji ROPD i urządzeń (HCI) serwerów zgodnie z załącznikiem H1.  Usługa obejmuje m.in. wykonywanie naprawy urządzeń z wykorzystaniem części zamiennych Zamawiającego i innych czynności określonych w pkt 9 bez wsparcia producenta. |
| SSD | Dysk półprzewodnikowy ([ang.](https://pl.wikipedia.org/wiki/J%C4%99zyk_angielski) solid-state drive, SSD) – pamięć masowa zbudowana w oparciu o [pamięć flash](https://pl.wikipedia.org/wiki/Pami%C4%99%C4%87_flash). |
| Subskrypcja | Umowa zawierana pomiędzy producentem / licencjodawcą a Zamawiającym, zapewniająca Zamawiającemu dostęp do produktu lub usługi i możliwość korzystania z tego produktu lub usługi przez określony okres, za stałą opłatą, pobieraną w cyklach rozliczeniowych; Subskrypcje na Oprogramowanie nie mogą ograniczać uprawnień Zamawiającego opisanych w Umowie. Musi zapewniać dostęp do wszystkich wymaganych Umową funkcjonalności w okresie jej obowiązywania. |
| Testy Odbiorcze | Testy wykonane zgodnie z Planem Testów wraz ze sprawdzeniem kompletności dostarczonych licencji w zakresie Oprogramowania i zakresu wykonanych prac. Pozytywny wynik Testów Odbiorczych stanowi jeden z warunków dokonania Odbioru prac zleconych. |
| Urządzenia | Sprzęt telekomunikacyjny i/lub teleinformatyczny, posiadany w ramach OSE i Systemu, m.in. serwery, macierze, przełączniki. |
| Ustawa OSE | Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej. |
| Usterka | Wystąpienie Problemu, który nie jest Awarią Istotną, Awarią Krytyczną, Awarią Poważną, zgodnie z zapisami pkt. 8 (Gwarancja) ppkt. 8.2. |
| Węzeł / Kolokacja / Obiekt / Lokalizacja | Miejsce fizyczne, powierzchnia kolokacyjna, w którym pracuje Węzeł sieci OSE / Węzeł Bezpieczeństwa OSE i umieszczone są serwery dla lokalizacji OPD i ROPD. |
| Węzeł bezpieczeństwa | Zespół urządzeń wraz z Oprogramowaniem, realizujących funkcje bezpieczeństwa sieciowego. |
| Węzeł sieci | Zespół urządzeń pracujących w jednej lokalizacji, zapewniających komunikację IP Użytkownikom sieci OSE z siecią Internet i podłączony węzeł bezpieczeństwa wraz z infrastrukturą Chmury Prywatnej. |
| Zwirtualizowana Infrastruktura Obliczeniowa (System) | Rozwiązanie informatyczne Zamawiającego w ramach Ogólnopolskiej Sieci Edukacyjnej, składające się z urządzeń i oprogramowania, dostarczające następujących funkcjonalności: chmura obliczeniowa w modelu SDDC (Software-Defined Data Center), Platforma Cloud Native, rozwiązania do przechowywania danych typu Storage i oprogramowania do zabezpieczania danych i ich archiwizacji (system kopii zapasowej). Całość stanowi kompleksowe rozwiązanie zapewniające przestrzeń do przechowywania i udostępniania usług wraz z elementami do automatyzacji, monitoringu, zarządzania i orkiestracji. |

# Chmura Prywatna

Zamawiający posiada prywatną chmurę obliczeniową składającą się m.in. z centralnych i regionalnych węzłów obliczeniowych, w których zainstalowane są urządzenia wraz z oprogramowaniem do wirtualizacji zasobów obliczeniowych w modelu SDDC, macierze do przechowywania kopii danych i system backupu. Uruchomiono w ten sposób strefy dostępności usług AZ-1 i AZ-2 zapewniając wysoką dostępność usług w ramach dwóch centralnych lokalizacji. Wdrożony i rozwijany od 2021 roku System, na który składa się Chmura Prywatna zapewnia w ramach OPD dostępność usług po awarii/niedostępności jednej z lokalizacji. Architektura Chmury Prywatnej w OPD operacyjnie zapewnia DR (Disaster Recovery) między lokalizacjami AZ-1 AZ-2. Trzecia lokalizacja AZ-3 stanowi infrastrukturę wspomagającą mechanizmy DR (Disaster Recovery), udostępniając możliwość automatyzacji w procesie przełączania usług m.in kworum, witness.

Całość posiadanego Systemu jako zwirtualizowana infrastruktura obliczeniowa zapewnia usługi i zasoby na potrzeby OSE. System podłączony jest do sieci OSE w 16 lokalizacjach Polski, czyli węzłach sieci OSE.

Schemat rozwiązania prezentuje rysunek poniżej:



### Platforma Konteneryzacyjna w ramach Chmury Prywatnej

Zamawiający w ramach Chmury Prywatnej posiada usługę orkiestracji klastrów Kubernetesowych w modelu Cloud Native które stanowi zintegrowane rozwiązanie SDDC uruchomione w centralnych lokalizacjach. Rozwiązanie wspiera i realizuje niezależność dostępności usług w AZ-1 i AZ-2 zapewniając dostępność lustrzanych usług w ramach dwóch centralnych lokalizacji. Platforma zapewnia obsługę pełnego cyklu operacyjnego od powołania po integracje, monitoring, aktualizacje jak również kasowanie wytworzonych klastrów Kubernetes wraz z wycofaniem konfiguracji/integracji.

# Opis przedmiotu zamówienia

### Opis ogólny

Przedmiotem zamówienia jest dostawa Oprogramowania i świadczenie usług w obszarze Chmury Prywatnej typu SDDC na potrzeby Ogólnopolskiej Sieci Edukacyjnej obejmujących: Serwis Gwarancyjny, Serwis Pogwarancyjny oraz wykonywanie Prac Zleconych i dostosowanie infrastruktury Chmury Prywatnej, zgodnie z wymaganiami opisanymi w dokumencie, a w szczególności:

1. Zapewnienie przez Wykonawcę Serwisu Gwarancyjnego (zgodnie z pkt 10, ze wsparciem producenta) dla Oprogramowania SDDC Chmury Prywatnej realizującego wirtualizacje zasobów obliczeniowych (m.in. compute storage network) i Platformy Kubernetesowej posiadanej w ramach Systemu (zwirtualizowanej infrastruktury obliczeniowej) dla lokalizacji OPD.
2. Dostarczenie przez Wykonawcę wymaganych licencji/subskrypcji w celu przedłużenia funkcjonowania Chmury Prywatnej w ramach Oprogramowania SDDC w OPD zgodnie z przedstawionymi w dokumencie warunkami.
3. Dostarczenie przez Wykonawcę wymaganych licencji/subskrypcji w celu przedłużenia funkcjonowania posiadanych funkcjonalności zapewniającej przenoszenie maszyn wirtualnych pomiędzy lokalizacjami w ramach ciągłości działania usług biznesowych Zamawiającego i Chmury Prywatnej (DR) opisanej w pkt. 5.4.
4. Dostosowanie przez Wykonawcę infrastruktury programowo-sprzętowej w OPD do zainstalowanego Oprogramowania SDDC w ramach Chmury Prywatnej do wymaganych zmian, wersji Oprogramowania SDDC i bieżących potrzeb Zamawiającego zgodnie z wymaganiami przedstawionymi poniżej w dokumencie.
5. Dostarczenie przez Wykonawcę Licencji i/lub Subskrypcji na Oprogramowanie SDDC zgodnego z aktualnie użytkowanymi urządzeniami HCI i oprogramowaniem Systemu:
   1. Serwery z rodziny PowerEdge R740 Dell Technologies,
   2. Serwery z rodziny PowerEdge R640 Dell Technologies,
   3. System backupu Dell Technologies Data Protection Suite NetWorker.
6. Zapewnienie przez Wykonawcę Serwisu Pogwarancyjnego (bez wsparcia producenta zgodnie z pkt 9) dla oprogramowania VMware w ROPD (m.in. Compute Storage) posiadanego w ramach Systemu w węzłach OSE.
7. Świadczenie przez Wykonawcę Serwisu Pogwarancyjnego dla posiadanych urządzeń Załącznik H1 - serwerów HCI w okresie Umowy realizowanego na częściach zamiennych Zamawiającego.
8. Świadczenie Serwisu Gwarancyjnego dla posiadanych wkładek optycznych 10Gbps i 40Gbps typu SFP+ i QSFP i baterii podtrzymujących konfiguracje serwerów dla Urządzeń - załącznik H1.
9. Świadczenie Prac Zleconych w okresie Umowy dla Oprogramowania i Urządzeń, zgodnie z przedstawionymi w dokumencie warunkami.
10. Realizacja praw Opcji w obrębie Oprogramowania i Urządzeń Chmury Prywatnej, zgodnie z przedstawionymi w dokumencie warunkami i Prac Zleconych.

### Opis Serwisu Gwarancyjnego

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do świadczenia Gwarancji w ramach dostarczonego Oprogramowania, integracji i realizacji Prac Zleconych w zakresie:

1. świadczenia Serwisu Gwarancyjnego w ramach Oprogramowania SDDC Chmury Prywatnej, Urządzeń w ramach Opcji i zrealizowanych Prac Zleconych, zgodnie z wymaganiami Zamawiającego opisanymi poniżej w dokumencie;
2. zapewnienie dostępu do aktualizacji oprogramowania, wsparcia technicznego producenta i gwarancyjnego dla posiadanego i dostarczonego Oprogramowania i Urządzeń;
3. zapewnienie wsparcia technicznego przez dziedzinowych inżynierów i architektów dla wykonywania zadań w okresie Umowy, na warunkach opisanych w niniejszym dokumencie;
4. zachowania funkcjonalności Chmury Prywatnej dla obszaru SDDC w ramach dostarczonego Oprogramowania - Chmury Prywatnej Zamawiającego w trakcie realizacji świadczenia usług Serwisu Gwarancyjnego i Prac Zleconych;
5. dostarczone Oprogramowanie dla OPD musi być kompatybilne z posiadanym i wykorzystywanym przez Zamawiającego oprogramowaniem i urządzeniami opisanymi w pkt 4.1 zapewniając przez przerwową prace usług i systemów uruchomionych w OPD i niezakłócone funkcjonowanie warstwy zarządzania lokalizacjami ROPD.
6. dostarczenie wymaganego Oprogramowania i umożliwienie zarządzania nim (m.in. licencjami, subskrypcjami) w oparciu o portal samoobsługowy producenta.
7. zapewnienia wsparcia technicznego w procesie eskalacji i koordynacji rozwiazywania zadań przekazywanych do wsparcia producenta Oprogramowania.
8. realizacji integracji w ramach Chmury Prywatnej w modelu SDDC, które będą obejmowały m.in.:
   1. implementacje Oprogramowania w ramach urządzeń Systemu (Załącznik H1);
   2. dostosowanie Oprogramowania do wymaganej nowej architektury potrzeb;
   3. reorganizacje/dostosowanie Oprogramowania w ramach Chmury Prywatnej OPD do zmian w architekturze rozwiązań SDDC producenta dostarczonego oprogramowania i wymagań licencyjnych zgodnie z pkt 5.;
9. realizacji Prac Zleconych w ramach Chmury Prywatnej i Opcji w modelu SDDC, które będą obejmowały m.in.:
   1. rekonfiguracje, implementacje, integracje Oprogramowania w ramach SDDC;
   2. realizację zadań w ramach składników SDDC i integracji:
      1. rekonfiguracje oprogramowania odpowiedzialnego za compute, storage, network, automatyzacje, orkiestracje, monitoring, administracje, raportowanie.
      2. implementacje zmian i nowych funkcjonalności
   3. dokumentowanie zmian w ramach wykonywanych zadań, prac zleconych, integracji, aktualizacja Dokumentacji Technicznej w zakresie przedmiotu Umowy;
   4. wdrożenie zmian dla Oprogramowania Chmury Prywatnej zgodnie z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną HLD i LLD;
   5. aktualizację procedur w zakresie: administracji, procedur eksploatacyjnych, awaryjnych w ramach przedmiotu Umowy;
   6. wsparcie w opracowaniu rozwiązań i ich implementacja w obszarze wirtualizacji centrów danych i Oprogramowania SDDC.
   7. zmian w zakresie sprzętu dla serwerów HCI w lokalizacjach OPD i ROPD obejmują m.in. relokacje urządzeń i elementów urządzeń np. dyski, kości pamięci RAM;
   8. uzyskanie akceptacji Zamawiającego w zakresie wykonanych zadań i Prac Zleconych.

### Opis Serwisu Pogwarancyjnego

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do świadczenia usług serwisu Pogwarancyjnego w ramach Urządzeń Systemu (Załącznik H1) w zakresie:

1. świadczenia usług wsparcia technicznego pogwarancyjnego dla oprogramowania VMware dla lokalizacji ROPD (wirtualizacja zasobów Compute i Storage) w ramach serwisu i Prac Zleconych, zgodnie z wymaganiami Zamawiającego;
2. świadczenia usług wsparcia technicznego pogwarancyjnego dla urządzeń HCI – serwerów zgodnych z punktem 9 w lokalizacjach OPD i ROPD, Wykonawca będzie wykonywał diagnostykę i naprawę urządzeń w 16 lokalizacjach Zamawiającego w oparciu o stan magazynowy Zamawiającego, na poczet realizacji usług pogwarancyjnych przeznaczonych zostanie minimum 10% urządzeń posiadanych - załącznik H1;
3. naprawa urządzeń będzie polegała na podmianie lub wymianie elementów urządzeń uszkodzonych i zastąpienie ich urządzeniami z zapasu magazynowego umieszczonego w 16 lokalizacjach ROPD i OPD - węzłach sieci OSE;
4. zapewnienie wsparcia technicznego w obszarze wymaganym przez dziedzinowych inżynierów doświadczonych w serwisie urządzeń posiadanych przez Zamawiającego;

### Założenia techniczne

Architektura posiadanego Systemu (zwirtualizowanej infrastruktury obliczeniowej) w zakresie Chmury Prywatnej Zamawiającego składa się z ponad 200 urządzeń typu HCI i serwerów dodatkowych zgodnie z załącznikiem H1.

W ramach Chmury Prywatnej w OPD Zamawiającego stosowane jest oprogramowanie VMware m.in.: vSphere, vSAN, VKS, NSX i pozostałe (m.in. vROPS, vRA, vRLI, vRNI, VIDM) zgodnie z bieżącą wersją VMware VCF 5.2 lub nowszą zgodnie z poniższą dok. producenta VMware Cloud Foundation 5.2 | 23 JUL 2024 | Build 24108943

[https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html /](https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html%20/) <https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-2/vcf-release-notes/vmware-cloud-foundation-52-release-notes.html>

W obszarze Platformy Kubernetesowej stosowane jest oprogramowanie do orkiestracji K8s VMware Tanzu Standard https://techdocs.broadcom.com/us/en/vmware-tanzu/standalone-components/tanzu-kubernetes-grid/2-5/tkg/index.html. Ekosystem SDDC zapewnia integracje i automatyzacje w zakresie operacyjnym dla Plaformy K8s w zakresie TKG/CCI, vRLI, vRA, vROPS.

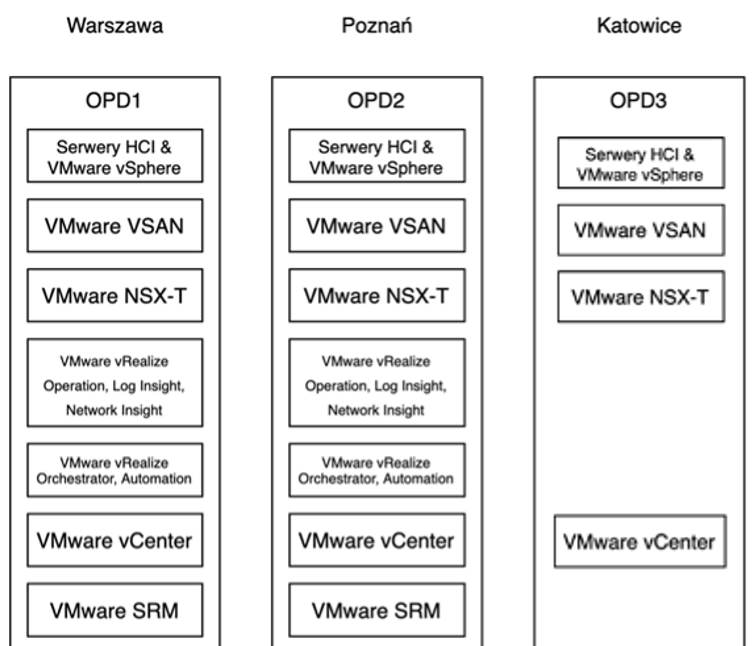
Regionalne węzły obliczeniowe ROPD posiadają urządzenia i oprogramowanie VMware w wersji HCI-KIT.

W obszarze kopii zapasowej i archiwum stosowane jest oprogramowanie Data Protection Suite – Backup & Recovery Software Dell Technologies [https://www.dell.com/en-us/shop/storage-servers-and-networking-for-business/sf/data-protection-suite.](https://www.dell.com/en-us/shop/storage-servers-and-networking-for-business/sf/data-protection-suite)

W obszarze zarządzanie sprzętem serwerowym jest to oprogramowanie OpenManage Enterprise Dell Technologies <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>.

Zastosowane komponenty oprogramowania prezentuje rysunek poniżej.

Obszar funkcjonalny OPD:

SDDC: 

Platforma K8s uruchomiona na zasobach SDDC: Obraz zawierający tekst, zrzut ekranu, diagram, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Obszar funkcjonalny ROPD:

Obraz zawierający tekst, Czcionka, zrzut ekranu, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Obszar funkcjonalny systemu Backupu – model poglądowy zabezpieczenia danych dla Chmury Prywatnej Zamawiającego. Schematy techniczne rozwiązania.

Obraz zawierający tekst, zrzut ekranu, diagram, Równolegle

Zawartość wygenerowana przez AI może być niepoprawna.

Topologia systemu backupu. Obraz zawierający tekst, diagram, linia, Czcionka

Zawartość wygenerowana przez AI może być niepoprawna.

Proces realizacji zabezpieczania danych.

Obraz zawierający tekst, diagram, zrzut ekranu, Plan

Zawartość wygenerowana przez AI może być niepoprawna.

### Wymagania w zakresie architektury

Umowa definiuje zakres usług i wymagania dla Oprogramowania Chmury Prywatnej w obszarze OPD. Wymagane jest dostarczenie licencji / subskrypcji w zakresie wymaganej pojemności, funkcjonalności na minimalny okres obowiązywania przedmiotu umowy. Realizacji opisanych w dokumencie usług.

Przedłużenie Serwisu Gwarancyjnego zgodnie z przedmiotem Umowy musi spełniać następujące wymagania Zamawiającego:

1. zgodność funkcjonalna dostarczonego Oprogramowania z obecnymi Urządzeniami Chmury Prywatnej, rozumiana jako kompatybilność posiadanej wersji oprogramowania i urządzeń (Załącznik H1) w tym wymienionym w pkt 3.1. Oferowane oprogramowanie musi znajdować się na liście zgodności z elementami Systemu wymienionymi w pkt 3.1.
2. wzajemna integracja dostarczonego Oprogramowania z obecnym Systemem/Chmurą Prywatną rozumiana jest jako niezakłócone stosowanie rozwiązań z pkt 3.1, narzędzi i aktualnego oprogramowania monitorującego wykorzystywanego przez Zamawiającego;
3. zapewnienie wymaganej ilości licencji / subskrypcji na dostarczane Oprogramowanie, z uwzględnieniem aspektów przełączania usług w przypadku awarii jednego z OPD, jeżeli jest wymagane;
4. wszystkie oferowane składniki Oprogramowania muszą być objęte Gwarancją zapewniając dostęp do wsparcia technicznego oraz Aktualizacji Oprogramowania co najmniej przez okres obowiązywania Umowy, lub okres wskazany dla Prawa Opcji;
5. realizacja Umowy i Prac Zleconych musi zostać zaplanowana i wykonana w modelu zapewniającym ciągłość działania całej Chmury Prywatnej Zamawiającego, zapewniając wysoką dostępność (HA) brak przerw operacyjnych w pracy Chmury Prywatnej i uruchomionych usług;
6. realizacja Umowy i Prac Zleconych musi wzorować się na architekturze referencyjnej producentów oferowanych rozwiązań i zgodności z integrowanym oprogramowaniem i sprzętem Zamawiającego opisanym w dokumentacji producentów;

### Skalowalność

Realizacja Umowy i Prac Zleconych nie może ograniczyć ani utrudniać realizacji zadań i dostępnych funkcjonalności w ramach posiadanej Chmury Prywatnej oraz musi zapewniać nadmiarowość zgodną z obszarami Chmury Prywatnej i Platformy Konteneryzacyjnej K8s, wynosić co najmniej N+1.

Uruchomienie nowego Oprogramowania nie może skutkować koniecznością wyłączenia obecnej infrastruktury i ograniczenia funkcjonalności, pojemności lub wydajności.

Proces uruchomienia Serwisu Gwarancyjnego musi być płynny i niezauważalny dla klienta końcowego.

# Zakres Umowy

Wymagania szczegółowe w zakresie objęcia Serwisem Gwarancyjnym i Pogwarancyjnym Chmury Prywatnej wraz z Oprogramowaniem i Urządzeniami zostały podzielone na poszczególne obszary i Opcje.

### Oprogramowanie stosowane w Chmurze Prywatnej

1. Zamawiający posiada następujące oprogramowanie funkcjonalne uruchomione w ramach Systemu:

Centralne lokalizacje:

* 1. Tabela produktów OPD:

|  |  |  |
| --- | --- | --- |
| Nazwa | P/N | Opis |
| VMware Cloud Foundation | VCF4-ADV-A | Pakiet VCF (Advance) – Vmware Cloud Foundation: vSphere Enterprise Plus, vSAN Advanced, NSX Data Center Advanced, vRealize Suite Enterprise, vRealize Network Insight Advanced, and SDDC Manager for vSAN.  Funkcjonalnie:  Wirtualizacja oraz HCI – vSphere Enterprise Plus 7 SDS – vSAN Advanced 7  SDN – NSX Advanced 3 Monitoring: vRealize Operations Enterprise (vRealize Suite Enterprise) Automatyzacja: vRealize Automation Enterprise (składowa vRealize Suite Enterprise) Logowanie: Log Insight (składowa vRealize Suite Enterprise) Monitoring sieci: vRealize Network Insight Advanced |
| Site Recovery Manager 8 Enterprise | VC-SRM8-25E-A | SRM 8 Ent. Licencja na replikację DR |
| VMware Tanzu Standard | TNZ-STD-COR-8X-TLSS-3Y-C | VMware Tanzu Standard Term Subscription + Production  Support for 3 year (per Core). |

Regionalne lokalizacje:

* 1. Tabela produktów ROPD:

|  |  |  |
| --- | --- | --- |
| Nazwa | P/N | Opis |
| HCI KIT Advanced | HCI-ADV-CPU-A | Oprogramowanie do wirtualizacji mocy obliczeniowej: HCI KIT Advanced:  VMware vSphere 7 Enterprise Plus for 1 processor and VMware vSAN 7 Advanced for 1 processor. Wirtualizacja i HCI |

1. W ramach obowiązujących umów dotyczących wdrożonego Systemu (m.in. Chmury Prywatnej) obecna gwarancja w zakresie Chmury Prywatnej w obszarze oprogramowania SDDC i Platformy Kontenerowej wygasa przed końcem 2025 roku.

### Serwery HCI stosowane w Chmurze Prywatnej

1. Zamawiający posiada w 16 lokalizacjach urządzenia HCI objęte licencjami VMware i są to serwery HCI zgodne z pkt 3.1 w liczbie:

Centralne lokalizacje:

* 1. Tabela ilościowa HCI OPD:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Ilość  HCI | ilość CPU w serwerze HCI | Liczba rdzeni CPU | Suma rdzeni w klastrze | Suma  Dysków Capacity | Suma  RAW ~ TiB |
| OPD MGMT | 1 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 280 | 45 | 322 |
| C2 | 2 | 1 | 28 | 56 | 10 | 58 |
| C3 | 2 | 2 | 24 | 96 | 0 | 0 |
| 2 |  |  |  |  |  |  |  |
| C2 | 5 | 2 | 28 | 280 | 45 | 322 |
| C2 | 2 | 1 | 28 | 56 | 10 | 58 |
| C3 | 2 | 2 | 24 | 96 | 0 | 0 |
| OPD PROD | 1 |  |  |  |  |  |  |  |
| C1 | 11 | 2 | 28 | 616 | 115 | 823 |
| C2 | 10 | 2 | 24 | 480 | 90 | 394 |
| 2 |  |  |  |  |  |  |  |
| C1 | 11 | 2 | 28 | 616 | 115 | 823 |
| C2 | 10 | 2 | 24 | 480 | 90 | 394 |
| 3 |  |  |  |  |  |  |  |
| C1 | 4 | 2 | 28 | 224 | 20 | 143 |
| OPT TEST | 1 |  |  |  |  |  |  |  |
| C1 | 6 | 2 | 28 | 336 | 66 | 472 |
|  |  | SUMA | 70 |  |  | 3616 | 606 | 3809 |

Dane ilościowe:

|  |  |
| --- | --- |
| SUMA Serwerów HCI | 70 |
| SUMA Capacity RAW vSAN ~TiB | 3809 |
| SUMA dysków Capacity | 606 |
| SUMA licencji VMware | 136 |
| SUMA rdzeni procesorów | 3616 |
| SUMA Procesorów - CPU | 136 |

Regionalne lokalizacje:

* 1. Tabela ilościowa HCI ROPD:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Ilość HCI | ilość CPU w serwerze HCI | Liczba rdzeni CPU | Liczba dysków 7,66TB Capacity w serwerze | Suma  Dysków Capacity | Suma  RAW ~ TiB |
| ROPD | 1 |  |  |  |  |  |  |  |
| C1 | 19 | 2 | 24 | 2 | 38 | 262 |
| C2 | 3 | 2 | 24 | 2 | 6 | 41 |
| 2 |  |  |  |  |  | 0 |  |
| C1 | 17 | 2 | 24 | 2 | 34 | 234 |
| C2 | 3 | 2 | 24 | 2 | 6 | 41 |
| 3 | C1 | 12 | 2 | 24 | 1 | 12 | 83 |
| 4 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 5 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 6 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 7 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 8 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 9 | C1 | 8 | 2 | 24 | 1 | 8 | 55 |
| 10 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 11 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 12 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 13 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 14 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 15 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| 16 | C1 | 7 | 2 | 24 | 1 | 7 | 48 |
| ROPD LAB | 1 | C1 | 4 | 2 | 24 | 3 | 12 | 83 |
| SUMA | | | 150 |  |  |  | 200 | 1379 |

Zamawiający posiada w każdych serwerze HCI dyski:

* Capacity typu SSD 7,68 TB | DELL EMC | SAS 12 Gbps,
* Cache typu Dell PowerEdge Express Flash NVMe 1,6TB,

Dane ilościowe:

|  |  |
| --- | --- |
| SUMA Serwerów HCI | 150 |
| SUMA Capacity RAW vSAN ~TiB | 1379 |
| SUMA dysków Capacity 7,66 TB | 200 |
| SUMA licencji VMware | 300 |
| SUMA rdzeni procesorów | 7200 |
| SUMA Procesorów - CPU | 300 |

### Docelowa architektura Chmury Prywatnej

Zamawiający wymaga dostosowania Chmury Prywatnej do zmian zgodnych z przedstawionymi poniżej wymaganiami:

1. Wykonanie rekonfiguracji Oprogramowania Chmury Prywatnej w terminie wymienionym poniżej od daty podpisania umowy, zgodnie z krokami poniżej opisanymi. Określony termin może zostać wydłużony, jeżeli wystąpią ograniczenia obiektywne po stronie Zamawiającego, o 4 tygodnie lub do czasu ustania przeszkód technicznych dla obszaru infrastruktury Zamawiającego.
2. Zamawiający wymaga aktywnej współpracy Architekta i Koordynatora zmiany z Zamawiającym w procesie wykonywania zmian.
3. Zamawiający zgodnie z planem prowadzenia prac będzie procesował wewnętrzne procesy przygotowując infrastrukturę i organizacje do wykonywania zmian.
4. Proces dostosowania Chmury Prywatnej zostanie poprzedzony przygotowaniem dokumentacji technicznej przez Wykonawcę, na podstawie zaakceptowanej dokumentacji technicznej (HLD i LLD) określającej zadania, sposób wykonywania zmian, proces zmian z harmonogram zadań zostaną przeprowadzone zmiany. Dokumentacja i zmiany mogę być wykonywane etapowo.
5. Dodatkowe zadania zlecone w ramach Prac Zleconych będą wykonywane przez Wykonawcę i zostaną zakończone w terminie określonym w pkt 7, jeżeli termin zadania nie został określony na inny przez Zamawiającego.

### Zamówienie podstawowe, pakiet Prac Zleconych

Wykonawca zobowiązuje się wykonywać zlecone zadania w obrębie Oprogramowania i serwerów HCI zwane Pracami Zleconymi na rzecz Zamawiającego. Zadania będą realizowane zgodnie z przedmiotem umowy na podstawie zleceń Zamawiającego.

1. Godziny zlecone będą to godziny poświęcone na prace inżynierów w zakresie zleconych zadań.
2. Godziny dojazdu i powrotu do lokalizacji nie są liczone dla lokalizacji OPD.
3. Podstawowy Pakiet godzin zleconych w okresie Umowy obejmuje:
   1. 800 godzin na rzecz Zamawiającego w obszarze oprogramowania,
   2. 150 godzin na rzecz Zamawiającego w obszarze sprzętu,
4. Zamawiający zgodnie z pkt 4.5, może pakiet godzin zleconych rozszerzyć o dodatkowe godziny zgodnie z Opcją AS i AH
5. Zakres zadań objętych pracami uszczegóławia opis z punktu 7.
6. Wykonawca będzie realizować zadania zlecone przez zespół inżynierów architektów posiadających odpowiednie umiejętności potwierdzone certyfikatami producentów Oprogramowania na poziomie min. profesjonalnym.
7. Doświadczenie Wykonawcy rozumiane jest jako praktyczne doświadczenie w zakresie wsparcia technicznego, implementacji i konfiguracji w obszarze Oprogramowania i rozwiązań SDDC.
8. Wykonawca będzie realizować zadania zlecone przez zespół inżynierów w którym co najmniej dwóch z nich będzie posiadało 3 letnie doświadczenie w obszarze sprzętu HCI objętego zadaniami zleconymi.

### Zamówienie Opcjonalne AS – rozszerzenie pakietu Prac Zleconych dla oprogramowania, 10 pakietów po 200 godzin

Wykonawca zobowiązuje się wykonać dodatkowy pakiet godzin w ramach obowiązującej Umowy, w zakresie pkt 4.4 i dotyczy zadań zleconych dla oprogramowania chmury dla lokalizacji OPD i ROPD.

### Zamówienie Opcjonalne AH – rozszerzenie pakietu Prac Zleconych dla sprzętu, 5 pakietów po 100 godzin

Wykonawca zobowiązuje się wykonać dodatkowy pakiet godzin w ramach obowiązującej Umowy, w zakresie pkt 4.4 i dotyczy zadań zleconych dla sprzętu wymienionego w załączniku H1.

# Docelowa architektura Chmury Prywatnej

Wykonawca w okresie Umowy, wykona zmiany w Chmurze Prywatnej OPD zgodnie z wymaganiami poniżej przedstawionymi, podzielonymi na etapy w celu optymalizacji procesu i zakresu zadań.

### Architektura Chmury Prywatnej – etap A

Wykonawca zobowiązuje się wykonać poniższe zadania w ciągu 18 tygodni od podpisania Umowy, zgodnie z wymaganiami:

1. Nie później jak w ostatnim tygodniu zostaną zakończone wymagane poniżej zadania i przeprowadzone testy odbiorcze potwierdzające zgodność zmian w wymaganiami etapu.
2. Aktywacja licencji i uruchomienie usługi Serwisu Gwarancyjnego dla Oprogramowania SDDC nastąpi w ciągu pięciu dni roboczych od zawarcia Umowy i nie wcześniej jak 18 grudnia 2025 r.
3. Wykonawca zgodnie z instrukcjami Zamawiającego przygotuje w ciągu pierwszych trzech tygodni od rozpoczęcia prac w zakresie Umowy Dokumentacje Techniczną (zawierającą HLD, LLD, harmonogram prac) wymaganych zmian dla etapu na podstawie wymagań i dokumentacji Systemu.
4. Zamawiający przy braku uwag zaakceptuje projekt techniczny opisujący wymagane zmiany (HLD, LLD, harmonogram) i zaakceptuje jego realizacje.

Uszczegółowienie wymagań dla etapu:

1. Zamawiający aktualnie posiada dwa Serwery zarządzające vCenter dla obszaru MGMT OPD1i2, kolejne dwa Serwery vCenter dla obszaru PRODUKCJA OPD1i2, jeden Serwer vCenter dla obszaru PRODUKCJA w OPD3 i jeden Serwer vCenter dla obszaru TEST OPT/ODP1.
2. Rekonfiguracja stanu obecnego do stanu docelowego obejmuje zmiany ilościowe uruchomionej WorkloadDomeny MGMT (obszaru zarządzania SDDC) dedykowanej do zarządzania infrastrukturą Chmury Prywatną w lok. OPD1 i OPD2 w ramach obecnej infrastruktury Systemu i uruchomionych rozwiązań wspomagających dla klastra C1, C3 i wycofanie C2, pkt 4.2.
   1. Zmiana liczby serwerów klaster C1 wraz z rekonfiguracjami obszar compute, SDN, SDS,
   2. Konsolidacja usług z klastra C2\* na rzecz klastrów C1 i C3,
3. Reorganizacja WorkloadDomeny MGMT dedykowanej funkcjom sieciowym i bezpieczeństwu sieciowemu, sieciom SDN.
   1. Reorganizacja klastra C3, zmiana liczby serwerów w klastrze, zapewnienie dodatkowego serwera typu Spare dla klastra, przełożenie kart sieciowych 40Gbps w obrębie całego klastra wraz z okablowaniem podłączeń,
   2. Relokacja urządzeń uzupełniających klaster wraz z okablowaniem,
   3. Reorganizacja usług SDN dla chmury prywatnej zgodnie z modelem licencyjnym i wymaganiami etapu.
      1. Przeniesienie bram P/V z klastra C1 i BareMetal Edge do zreorganizowanego klastra C3.
      2. Uruchomienie usług bezpieczeństwa sieciowego dla obszaru OPT i MGMT (IPS/IDS, URL-Filtering),
      3. Uruchomienie analityki monitorującej zdarzenia dla obszaru NG-Firewall w zakresie usług bezpieczeństwa sieciowego w SDN.
4. Uruchomienie funkcjonalności umożliwiającej udostępnianie przestrzeni dyskowej DataStore w klastrze SDS pomiędzy klastrami MGMT w obrębie lokalizacji.
5. Rekonfiguracja stanu obecnego do stanu docelowego obejmujące zmiany ilościowe uruchomionej WorkloadDomeny PRODUKCJA dedykowanej dla usług w Chmurze SDDC w lok. OPD1 i OPD2 w ramach obecnej infrastruktury i uruchomionych rozwiązań Klaster C1 i C2, pkt 4.2.
6. Dostosowanie posiadanej funkcjonalności orkiestracji klastrów Kubernetesowych w obu klastrach PRODUKCYJNYCH C2 do zmian w Oprogramowaniu.
7. Uruchomienie funkcjonalności umożliwiającej wzajemne udostępnianie przestrzeni dyskowej DataStore w klastrze SDS pomiędzy klastrami PRODUKCYJNYMI w obrębie lokalizacji.
8. Dostosowanie funkcjonalności replikacji DataStore maszyn wirtualnych pomiędzy lokalizacjami wraz z orkiestracją procesu DR pomiędzy lokalizacjami OPD1 i OPD2.
9. Dostosowanie narzędzi zarządzania usługami w ramach stosu Chmury Prywatnej SDDC zgodnie z dostarczonym Oprogramowaniem i zmianami wyżej wymienionymi, m.in. aktualizacja zadań/czynności w obszarze katalogu usług, automatyzacji, orkiestracji i monitoringu do stanu docelowego w tym narzędzi bazujących na skryptach.
10. Stan docelowy infrastruktury chmury prywatnej dla tego etapu prezentują schematy poniżej:
    1. Schemat topologiczny klastrów obliczeniowych obszar MGMT

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* 1. Schemat topologiczny klastrów obliczeniowych obszar PRODUKCJA i TEST

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. Liczba i zakres ilościowy serwerów HCI ulega zmianie dla klastrów: MGMT C1, C3 PRODUKCJA C1 i TEST(OPT) C1.
  1. Schemat zmian dla obszaru funkcjonalnego SDN w SDDC Chmury OSE prezentuje nowy klaster C3, odpowiedzialny za P/V, usługi sieciowe w tym bezpieczeństwa te lokalne i między lokalizacjami.

Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. Bramy komunikacyjne P/V, odpowiedzialne za komunikacje Overlay z Underlay dla SDN zostaną uruchomione na dedykowanym klastrze w obszarze WD-MGMT zapewniających rezerwowane zasoby obliczeniowe na rzecz usług sieciowych i Advanced NG-Firewall.
    2. Funkcje P/V zostaną ulokowane w sposób zapewniający gwarancje zasobów obliczeniowych dla usług krytycznych.
  1. Sieć SDN musi zapewniać następujące punkty wymiany ruchu IP pomiędzy Overlay z Underlay zaprezentowane poniżej na schemacie.
     1. Obszar funkcjonalny MGMT przedstawia schemat poniżej.

Obraz zawierający tekst, zrzut ekranu, Czcionka, logo

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. Obszar funkcjonalny PRODUKCJA przedstawia schemat poniżej.

Obraz zawierający Jaskrawoniebieski, zrzut ekranu, niebieskie, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. Obszar funkcjonalny TEST przedstawia schemat poniżej.

Obraz zawierający tekst, zrzut ekranu, Prostokąt, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. W sieci Zamawiającego występują Bramy P/V łączące świat wirtualnych sieci (SDN) z fizycznymi urządzeniami sieciowymi, które realizującą m.in. funkcjonalności routingu IP, kontroli ruchu IP (Firewall). Przedstawiony powyżej schemat prezentuje wymaganą liczbę punktów styku P/V z funkcjonalnościami NG-Firewall, routing IP i usług bezpieczeństwa sieciowego (Network Security: IPS/IDS, URL-Filtering, Malware).
    2. Wymagane klastry P/V SDN podzielone są na klastry lokalne występujące wyłącznie w jednej lokalizacji jak i w dwóch zapewniając przełączanie – przenoszenie usług pomiędzy lokalizacjami w ramach m.in. HA i DR. Całościowy model rozwiązania prezentuje schemat poniżej.

Obraz zawierający zrzut ekranu, diagram, design

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

1. Sprzęt HCI zastosowany do obsługi wymaganych funkcjonalności zostanie ograniczony i będzie następujący:
   1. Tabela z zestawieniem ilościowym obszar compute i storage:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Ilość  HCI | ilość CPU w serwerze HCI | Liczba rdzeni CPU | Suma Rdzeni w klastrze | Suma  Dysków Capacity | Suma  RAW ~ TiB |
| OPD MGMT | 1 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 224 | 44 | 290 |
|  |  |  |  |  |  |  |
| C3 | 3 | 2 | 24 | 144 | 0 | 0 |
| 2 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 224 | 44 | 290 |
|  |  |  |  |  |  |  |
| C3 | 3 | 2 | 24 | 144 | 0 | 0 |
| OPD PROD | 1 |  |  |  |  |  |  |  |
| C1 | 8 | 2 | 28 | 448 | 80 | 538 |
| C2 | 10 | 2 | 24 | 480 | 90 | 394 |
| 2 |  |  |  |  |  |  |  |
| C1 | 8 | 2 | 28 | 448 | 80 | 538 |
| C2 | 10 | 2 | 24 | 480 | 90 | 394 |
| 3 |  |  |  |  |  |  |  |
| C1 | 4 | 2 | 28 | 224 | 20 | 132 |
| OPT TEST | 1 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 280 | 60 | 395 |
| SUMA | | | 59 |  |  | 3096 |  | 3078 |

* 1. Tabela z zestawieniem ilościowym funkcjonalności Network Security w ramach SDN:

|  |  |  |  |
| --- | --- | --- | --- |
| Obszar | Lok. | Klaster | SDN Advanced NG-Firewaling L2-L7 na poziomie vNIC VM - wirtualnej karty sieciowej podłączonej dla maszyny wirtualnej |
|  |
| OPD MGMT | 1 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
|  |  |  |
| C3 | n.d. |  |
| 2 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
|  |  |  |
| C3 | n.d. |  |
| OPD PROD | 1 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| C2 | Obsługa NG-Firewall dla vNIC VM |  |
| 2 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| C2 | Obsługa NG-Firewall dla vNIC VM |  |
| 3 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| OPT TEST | 1 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| Suma rdzeni CPU | | | 2808 |

* 1. Tabela z zestawieniem ilościowym Network Security – SDN dla bram komunikacyjnych P/V:

|  |  |  |  |
| --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Suma vCPU dla P/V SDN z funkcjonalnością  Advanced NG-Firewaling L2-L7 |
| OPD MGMT | 1 |  |  |
| C1 | 24 |
| C3 |
| 2 |  |  |
| C1 | 24 |
| C3 |
| OPD PROD | 1 |  |  |
| C1 | 64 |
| C2 |
| 2 |  |  |
| C1 | 64 |
| C2 |
| 3 |  |  |
| C1 | 32 |
| OPT TEST | 1 | C1 | 48 |
| 2 |  |  |
|  |  |  |  |
| Bramy P/V suma wymaganej liczby rdzeni vCPU | |
| Advanced NG-Firewall | **256** |

* 1. Przygotowanie Testów Odbiorczych (planu i dokumentacji) przez Wykonawcę zgodnie z zakresem etapu i wytycznymi Zamawiającego m.in.
     1. Testy funkcjonalne Chmury Prywatnej po zmianach dla etapu zgodne z wymaganiami i zgodność z dokumentacją techniczną (HLD i LLD).
        1. Kryterium sukcesu brak rozbieżności konfiguracji Chmury Prywatnej z przygotowaną dokumentacją HLD i LLD i wymaganiami niniejszego dokumentu.
     2. Testy ilościowe weryfikacja zgodności uruchomionych licencji dla Chmury Prywatnej OPD z ofertą (BOM) dostarczonymi licencjami.
        1. Kryterium sukcesu brak rozbieżności ilościowych.
     3. Testy zachowania mechanizmów DR / HA ciągłości działania lok. OPD.
        1. Wykonanie kontrolowanego procesu wyłączenia jednej z lokalizacji OPD1 lub ODP2 i weryfikacja ciągłości działania Chmury Prywatnej w zakresie zarządzania wymaganymi składnikami oprogramowania SDDC i dostępności usług posiadanych na obecnym Systemie.
           1. Kryterium sukcesu dostępność Chmury Prywatnej i uruchomionych usług Zamawiającego po wyłączeniu jednej lokalizacji.
           2. Kryterium sukcesu skuteczne uruchomienie wyłączonej lokalizacji Chmury Prywatnej bez błędów i awarii na funkcjonowanie włączonej lokalizacji.
     4. Testy potwierdzające zachowanie obecnych funkcjonalności Chmury Prywatnej po zmianach.
        1. Funkcjonalności posiadanego oprogramowania odpowiedzialnego za monitorowanie alertowanie i raportowania zdarzeń w ramach posiadanych narzędzi Chmury Prywatnej.
           1. Kryterium sukcesu dostępność narzędzi i danych odbieranych z Chmury Prywatnej po zakończeniu etapu.
        2. Kontynuacja funkcjonowania mechanizmów kontroli ruchu IP w sieci SDN na poziomie vNIC (karty sieciowej VM) i bramy komunikacyjnej P/V:
           1. Testy wymagane potwierdzające funkcjonalności IPS / IDS / URL-Filtering (emulowanie realnych zagrożeń i analiza funkcjonowania wymaganych mechanizmów bezpieczeństwa sieciowego m.in. konfiguracja wymaganej kontroli i przeprowadzenie prób kontrolowanego naruszenia bezpieczeństwa

Kryterium sukcesu to zaprezentowania działania mechanizmów rozpoznawania i kontroli dla przykładowego ataku i konfiguracji dla wymaganych mechanizmów.

* + - * 1. Test dostarczonych narzędzi analitycznych dla ww. funkcjonalności kontroli bezpieczeństwa sieciowego w SDN, realne zaprezentowanie funkcjonowania oprogramowania przy próbach zagrożeń mogących naruszający bezpieczeństwo danych i systemów.

Kryterium sukcesu to zaprezentowanie narzędzi raportujących dla przykładowych zagrożeń.

* + - 1. Katalog usług, automatyzacji, orkiestracji zadań.
         1. Kryterium sukcesu to dostępność posiadanych mechanizmów po zmianach i dostosowanie ich działania do zmian.
      2. Integracji z systemami zewnętrznymi m.in. Solarwinds, Zabbix.
  1. Wykonanie Testów Odbiorczych przez Wykonawcę przy udziale Zamawiającego weryfikujących wymagane zmiany i funkcjonalności Chmury dla etapu, zgodność z wymaganiami, HLD i LLD.
  2. Uzyskanie akceptacji Zamawiającego dla wyników testów odbiorczych, zgodności z BOM, braku błędów i awarii w zakresie funkcjonalności Oprogramowania.

Powyższy etap dostosowuje Chmurę Prywatną OPD do wymaganych zmian w ramach dostarczonego Oprogramowania SDDC przez Wykonawcę.

### Architektura Chmury Prywatnej – etap B, kontynuacja zmian z etapu A

Wykonawca zobowiązuje się wykonać poniższe zadania do 20 września 2026 r., zgodnie z wymaganiami:

1. Aktywacja wymaganych licencji nastąpi nie później jak 1 września 2026 r.
2. Wykonawca zgodnie z instrukcjami Zamawiającego przygotuje do 30 czerwca 2026 roku aktualizacje Dokumentacji Technicznej (HLD, LLD, harmonogram) wymaganych zmian dla etapu na podstawie wymagań i dokumentacji Chmury Prywatnej.
3. Zamawiający przy braku uwag zaakceptuje Dokumentacje Techniczną opisującą wymagane zmiany (HLD, LLD, harmonogram) i zaakceptuje jego realizacje.

Uszczegółowienie wymagań dla etapu:

1. Uruchomienie funkcjonalności orkiestracji klastrów Kubernetesowych dla pozostałych klastrów w OPD: PRODUKCJA C1, MGMT C1 i TEST C1 wraz integracjami na poziomie ich orkiestracji, automatyzacji i monitoringu.
2. Rekonfiguracja w tym ilościowa WorkloadDomeny PRODUKCYJNEJ C2 Chmurze SDDC w lok. OPD1 i OPD2 do docelowej skali.
3. Uruchomienie nowego wysoce wydajnego zasobu dyskowego SDS dla klastrów C2 w PRODUKCJI bazującego na dyskach NVMe i udostępnienie jego przestrzeni do klastrów PRODUKCYJNYCH w obrębie lokalizacji OPD.
4. Rekonfiguracja w tym ilościowa uruchomionej WorkloadDomeny PRODUKCJA zgodnie z tabelą poniżej.
5. Rekonfiguracja i rozbudowa obszaru WorkloadDomeny TEST do docelowego modelu zgodnie z Oprogramowaniem:
   1. Reorganizacja WorkloadDomeny TEST w obrębie obszaru OPT1.
   2. Zaprojektowanie i implementacja nowej WorkloadDomeny TEST jako obszar OPT2 analogicznie do istniejącego obszaru OPT1.
   3. Uruchomiona lokalizacja OPT2 będzie w pełni funkcjonalna i samodzielna po wyłączeniu lok. OPT1.
6. Rekonfiguracja sieci SDN dla Chmury Prywatnej i pełne wdrożenie funkcjonalności bezpieczeństwa sieciowego zgodnie z wymaganiami i Oprogramowaniem:
   1. Dostosowanie konfiguracji Chmury Prywatnej do zmian w Oprogramowaniu SDN.
   2. Uruchomienie rozproszonego i zcentralizowanego bezpieczeństwa sieciowego w SDN obejmującego funkcjonalności Advanced NG-Firewall (IPS IDS URL Filtering Malware) dla MGMT, PRODUKCJA, TEST.
      1. Analiza i wdrożenie funkcjonalności IDS.
      2. Analiza i wdrożenie funkcjonalności IPS.
      3. Analiza i wdrożenie funkcjonalności URL-Filtering wraz z dostosowaniem do potrzeb.
      4. Analiza i wdrożenie funkcjonalności Malware Protection dla TESTu (OPT1 i OPT2).
   3. Przygotowanie widoków, raportów i alertów dla monitorowania i analizy zagrożeń sieciowych dla ww funkcjonalności.
   4. Integracja OPT2 z SDN dla WorkloadDomeny TEST.
7. Uruchomienie monitorowania komunikacji sieciowej w obrębie posiadanych namespace / klastrów K8s, wdrożenie kontroli dla ruchu wejściowego i wyjściowego w obrębie każdego klastra na podstawie zbieranych danych pomiarowych przepływów IP w ramach klastrów / namespaces.
8. Dostosowanie oprogramowania zarządzającego usługami w ramach Chmury SDDC zgodnie ze zmianami wyżej wymienionymi, m.in. aktualizacja zadań/czynności w obszarze katalogu usług, automatyzacji, orkiestracji i monitoringu-raportowania.
9. Przeprowadzenie dwóch instruktarzy z zawansowanego monitoringu zagrożeń i analizy włamań dla zaawansowanych funkcjonalności SDN Advanced NG-Firewaling L2-L7 minimum 10 osób.
   1. Omówienie ww. funkcjonalności bezpieczeństwa w SDN.
   2. Przykłady i pokaż funkcjonalności na podstawie WD-TESTu OPT1/2.
   3. Laboratoria praktyczne m.in. w OPT.
   4. Czas trwa - minimum 16 godzin.
   5. Dostarczenie materiałów szkoleniowych zgodnych z oficjalnymi materiałami producenta.
10. Rozwiązanie docelowe dla tego etapu prezentują schematy poniżej:
    1. Schemat topologiczny klastrów obliczeniowych obszar PRODUKCJA i TEST

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. Obszar WD-TEST zostanie rozbudowany o 4 serwery HCI w lokalizacji OPT2 (OPD2).
  1. Schemat wymagań dla funkcjonalności Oprogramowania SDN w Chmurze OSE zostanie rozbudowany o lokalizacje OPT2 i zmiany niezbędne dla obszaru OPT1.
     1. Nowe Bramy komunikacyjne P/V, odpowiedzialne za komunikacje Overlay z Underlay w SDN TEST OPT zostaną uruchomione na dedykowanym klastrze C3 WD-MGMT zapewniających zasoby obliczeniowe.
  2. Sieć SDN musi zapewniać następujące punkty wymiany ruchu IP pomiędzy Overlay z Underlay zaprezentowane poniżej na schemacie.
     1. Obszar funkcjonalny TEST przedstawia schemat poniżej.

Obraz zawierający zrzut ekranu, Jaskrawoniebieski, design

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. W sieci SDN występują bramy komunikacyjne obsługujące funkcjonalności NG-Firewall i sam routing IP (bez funkcjonalności Firewall / kontroli IP-ACL i usług bezpieczeństwa sieciowego m.in. IPS/IDS) dedykowane dla obszaru TEST- DEV.
    2. Klastry podzielone są na klastry lokalne występujące wyłącznie w jednej lokalizacji jak i klastry w dwóch lokalizacjach zapewniając przełączanie – przenoszenie usług pomiędzy lokalizacjami.

1. Sprzęt HCI zastosowany do obsługi wymaganych funkcjonalności będzie następujący:
   1. Tabela z zestawieniem ilościowym obszar Compute i Storage:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Ilość  HCI | ilość CPU w serwerze HCI | Liczba rdzeni CPU | Suma Rdzeni w klastrze | Suma  Dysków Capacity | Suma  RAW ~ TiB |
| OPD MGMT | 1 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 224 | 44 | 290 |
|  |  |  |  |  |  |  |
| C3 | 3 | 2 | 24 | 144 | 0 | 0 |
| 2 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 224 | 44 | 290 |
|  |  |  |  |  |  |  |
| C3 | 3 | 2 | 24 | 144 | 0 | 0 |
| OPD PROD | 1 |  |  |  |  |  |  |  |
| C1 | 8 | 2 | 28 | 448 | 80 | 538 |
| C2 | 88 | 2 | 24 | 384384 | 7272 | 17317 |
| 2 |  |  |  |  |  |  |  |
| C1 | 8 | 2 | 28 | 448 | 80 | 538 |
| C2 | 88 | 2 | 24 | 384384 | 7272 | 17317 |
| 3 |  |  |  |  |  |  |  |
| C1 | 4 | 2 | 28 | 224 | 20 | 132 |
| OPT TEST | 1 |  |  |  |  |  |  |  |
| C1 | 5 | 2 | 28 | 280 | 60 | 395 |
| 2 | C2 | 4 | 2 | 24 | 192 | 3 | 79 |
| SUMA | | | **59** |  |  | **3096** |  | **2893** |

* 1. Tabela zestawieniem ilościowym funkcjonalności Network Security w ramach SDN:

|  |  |  |  |
| --- | --- | --- | --- |
| Obszar | Lok. | Klaster | SDN Advanced NG-Firewaling L2-L7 na poziomie vNIC VM - wirtualnej karty sieciowej maszyny wirtualnej |
|  |
| OPD MGMT | 1 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
|  |  |  |
| C3 | n.d. |  |
| 2 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
|  |  |  |
| C3 | n.d. |  |
| OPD PROD | 1 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| C2 | Obsługa NG-Firewall dla vNIC VM |  |
| 2 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| C2 | Obsługa NG-Firewall dla vNIC VM |  |
| 3 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| OPT TEST | 1 |  |  |  |
| C1 | Obsługa NG-Firewall dla vNIC VM |  |
| 2 | C1 | Obsługa NG-Firewall dla vNIC VM |  |
| Suma rdzeni CPU | | | 2808 |

* 1. Tabela z zestawieniem ilościowym Network Security – SDN dla bram komunikacyjnych P/V:

|  |  |  |  |
| --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Suma vCPU dla P/V SDN z funkcjonalnością Advanced NG-Firewaling L2-L7 |
| OPD MGMT | 1 |  |  |
| C1 | 24 |
| C3 |
| 2 |  |  |
| C1 | 24 |
| C3 |
| OPD PROD | 1 |  |  |
| C1 | 64 |
| C2 |
| 2 |  |  |
| C1 | 64 |
| C2 |
| 3 |  |  |
| C1 | 32 |
| OPT TEST | 1 | C1 | 64 |
| 2 | C2 | 48 |
|  |  |  |  |
| Bramy P/V suma wymaganej liczby rdzeni vCPU | |
| Advanced NG-Firewall | **320** |

* 1. Przygotowanie Testów Odbiorczych przez Wykonawcę zgodnie z zakresem etapu i wytycznymi Zamawiającego m.in.
     1. Testy funkcjonalne Chmury Prywatnej obejmujące zrealizowane zmiany zgodne z wymaganiami Umowy.
        1. Kryterium sukcesu zgodność konfiguracji Chmury Prywatnej z Dokumentacją Techniczną.
     2. Testy ilościowe zgodnie z ofertą (BOM).
        1. Kryterium sukcesu zgodność liczby licencji uruchomionych ze stanem licencji BOS.
     3. Testy potwierdzające uruchomienie lokalizacji OPT2 zgodnie z Dokumentacją Techniczną.
        1. Kryterium sukcesu zgodność konfiguracji OPT2 z Dokumentacją Techniczną.
     4. Testy mechanizmów DR / HA ciągłości działania dla lok. OPT1 i OPT2.
        1. Kryterium sukcesu test potwierdzający funkcjonowania mechanizmów HA w ramach lok i dostępność mechanizmów DR po wyłączeniu lokalizacji OPT2.
     5. Testy potwierdzające wymagane funkcjonalności dla zrealizowanych zadań m.in. OPT.
        1. Funkcjonalności monitoringu (alertowania i raportowania).
        2. Kryterium sukcesu otrzymywanie alertów i alarmów po wywołaniu anomalii w dla lokalizacji OPT
        3. Monitoring w zakresie SDN Advance Security NG-Firewall / IDS / IPS / URL-Filtering / Malware Protection.
        4. Kryterium sukcesu zaprezentowanie funkcjonowania ww mechanizmów bezpieczeństwa sieciowego.
        5. Rozbudowa katalogu usług, automatyzacji, orkiestracji zadań w zakresie zmian.
        6. Kryterium sukcesu zgodność funkcjonowania katalogu usług z zakresem wykonanych zmian.
        7. Integracja z systemami zewnętrznymi m.in. Solarwinds, Zabbix.
  2. Wykonanie Testów Odbiorczych przez Wykonawcę przy udziale Zamawiającego weryfikujących wymagane zmiany i funkcjonalności Chmury dla etapu.
  3. Uzyskanie akceptacji Zamawiającego dla wyników testów odbiorczych, zgodności z BOM, braku błędów i awarii.

Ostatni etap zmian obejmuje reorganizacje infrastruktury Chmury Prywatnej OPD do zmian docelowych.

### Architektura Chmury Prywatnej – etap C

Wykonawca zobowiązuje się wykonać poniższe zadania zgodnie z wymaganiami do 20 marca 2027 roku.

1. Aktywacja wymaganych licencji nastąpi nie później jak 31 stycznia 2027 r.
2. Wykonawca zgodnie z instrukcjami Zamawiającego przygotuje do 30 listopada 2026 roku aktualizację Dokumentacji Technicznej (HLD, LLD, harmonogram) wymaganych zmian dla etapu na podstawie wymagań, konsultacji z Zamawiającym i dokumentacji Chmury Prywatnej z etapu A i B.
3. Zamawiający przy braku uwag zaakceptuje Dokumentacje Techniczną opisujący wymagane zmiany w zakresie aktualizacji (HLD, LLD, harmonogram) i zaakceptuje jego realizacje.

Uszczegółowienie wymagań dla etapu:

1. Dostosowanie narzędzie realizujących proces DR - zapewniających migracje/przenoszenie maszyn wirtualnych pomiędzy lokalizacjami dla lokalizacji ODP1 i OPD2 w ramach wymaganej liczby licencji.
2. Wykonanie zmian w stosie technologicznym SDDC w obszarze PRODUKCJA, MGMT i TEST celem dostosowania do bieżącej wersji Oprogramowania.
   1. Zaprojektowanie docelowego modelu architektury Chmury Prywatnej zgodnie z wersją Oprogramowania i wymaganiami Zamawiającego.
   2. Uzyskanie zgody Zamawiającego dla procesu zmian dostosowujących infrastrukturę Chmury Prywatnej.
   3. Realizacja procesu przebudowa Chmury Prywatnej do zmian wymaganych w ramach zatwierdzonego dokumentacji.
3. Rekonfiguracja i migracja zgodnie projektem i wymaganiami Oprogramowania do docelowego modelu Chmury Prywatnej obejmuje m.in.:
   1. Uruchomienie infrastruktury docelowej SDDC w obszarze compute, SDS, SDN.
   2. Migracja i integracja narzędzi SDDC.
   3. Migracja zaawansowanego bezpieczeństwa sieciowego SDN wraz z systemami zamawiającego.
   4. Implementacja bezpieczeństwa sieciowego w obszarze Malware Protection i zaawansowanego monitoringu i wykrywania zagrożeń dla całości Chmury SDDC.
   5. Dostosowanie narzędzi monitoringu, raportosowania po zmianach i przygotowanie co najmniej 50 konfiguracji zgodnie z potrzebami Zamawiającego (obszar cyklicznych raportów, widoków prezentujących aktualne dane, alertów dynamicznie generowanych powiadomień po przekroczeniu zdefiniowanych progów dla stanu Chmury SDDC i uruchomionych usług)
4. Wdrożenie bezpieczeństwa sieciowego w SDN Chmury OSE obejmie:
   1. Aktywne monitorowanie IPS, IDS, URL-Filtering,
   2. Malware protection i analityki w zakresie wykrywania niebezpiecznych działań zapobiegając infekcjom złośliwym kodem, takim jak wirusy, ransomware czy spyware i analizy wektorów ataku po infekcji.
   3. Uruchomienie agentowego monitoringu maszyn wirtualnych w oparciu o oprogramowanie vROPS lub równoważne zapewniając zbieranie metryk w zakresie pracy maszyn wirtualnych wykonywanie analiz i alarmowanie.
   4. Uruchomienie agentowego monitoringu maszyn wirtualnych w oparciu o oprogramowanie vRLI lub równoważne zapewniając zbieranie logów audytowych i zdarzeń występujących na poziomie maszyn wirtualnych i ich analizę i alarmowanie.
5. Migracja posiadanych rozwiązań w ramach infrastruktury Zamawiającego:
   1. Przeniesienie stanu przygotowanych integracji, automatyzacji, konfiguracji i monitoringu po zmianach.
   2. Dostosowanie procedur do zmian w stosie SDDC.
   3. Dostosowanie posiadanych rozwiązań do potrzeb Zamawiającego.
6. Rozwiązanie docelowe finalne prezentują schematy poniżej:
   1. Schemat topologiczny klastrów obliczeniowych.

Obraz zawierający tekst, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. Sprzętowy stos technologiczny urządzeń zostanie dostosowany przez Zamawiającego do potrzeb architektury Oprogramowania (np. ilość zasobów dyskowych).
    2. Obszar rozwiązań Kubernetesowych zostanie rozbudowany do stanu poniżej:

Obraz zawierający tekst, zrzut ekranu, design

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* 1. Sieć SDN zapewni zaawansowane bezpieczeństwo i kontrole komunikacji.
     1. Schemat sieci SDN w obszarze P/V.

Obraz zawierający zrzut ekranu, tekst, diagram, design

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

* + 1. W sieci SDN będą występowały bramy komunikacyjne P/V obsługujące funkcjonalności NG-Firewall i sam routing IP zgodnie ze schematem.
    2. Klastry rozciągnięte pomiędzy OPD1 i OPD2 zapewniają przenoszenie usług pomiędzy lokalizacjami bez zmiany adresacji IP usług relokowanych z OPD1 do OPD2 lub OPD2 do OPD1.

1. Sprzęt HCI zastosowany do obsługi wymaganych funkcjonalności będzie następujący:
   1. Tabela z zestawieniem ilościowym obszar Compute i Storage:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Ilość HCI | Rdzenie w klastrach | RAW SDS ~ TiB |
| **SUMA** | **59** | **3096** | **3000** |

* 1. Tabela zestawieniem ilościowym funkcjonalności Network Security w ramach SDN:

|  |  |  |  |
| --- | --- | --- | --- |
| Obszar | Lok. | Klaster | SDN Advance NG-Firewaling L2-L7 na poziomie vNIC VM- wirtualnej karty sieciowej podłączonej do maszyny wirtualnej |
|  |
| Suma rdzeni CPU | | | 2808 |

* 1. Tabela z zestawieniem ilościowym Network Security – SDN dla bram komunikacyjnych P/V:

|  |  |  |  |
| --- | --- | --- | --- |
| Obszar | Lok. | Klaster | Suma vCPU dla P/V SDN z funkcjonalnością  Advanced NG-Firewaling L2-L7 |
| OPD MGMT | 1 |  |  |
| C1 | 24 |
| C3 |
| 2 |  |  |
| C1 | 24 |
| C3 |
| OPD PROD | 1 |  |  |
| C1 | 96 |
| C2 |
| 2 |  |  |
| C1 | 96 |
| C2 |
| 3 |  |  |
| C1 | 32 |
| OPT TEST | 1 | C1 | 64 |
| 2 | C2 | 48 |
|  |  |  |  |
| Bramy P/V suma wymaganej liczby rdzeni vCPU | |
| Advanced NG-Firewall | **384** |

* 1. Przygotowanie Testów Odbiorczych przez Wykonawcę zgodnie z zakresem etapu wytycznymi Zamawiającego m.in.
     1. Testy funkcjonalne Chmury Prywatnej po zmianach zgodne z wymaganiami poniżej.
     2. Testy ilościowe zgodnie z ofertą (BOM).
        1. Kryterium sukcesu zgodność zastosowanej liczby licencji z zamówieniem.
     3. Testy mechanizmów DR / HA ciągłości działania Chmury Prywatnej.
        1. Kryterium sukcesu dostępność zarządzania i narzędzi Chmury Prywatnej i usług uruchomionych po wyłączeniu jednej z lokalizacji OPD1 lub OPD2.
        2. Kryterium sukcesu dostępność usług po awarii jednego z urządzeń nadmiarowych dla co najmniej 10 testów.
        3. Kryterium sukcesu dostępność usług po awarii jednego z elementów nadmiarowych dla Oprogramowania SDDC co najmniej 5 testów.
     4. Testy potwierdzające funkcjonalności Chmury Prywatnej po zmianach.
        1. Mechanizmów DR przenoszenia usług pomiędzy lokalizacjami i dostępności usług po wyłączeniu jednej lokalizacji: OPD1 i OPD2.
           1. Kryterium sukcesu dostępność usług po wykonaniu wymaganych ww testów.
        2. Funkcjonalności monitoringu (alertowania i raportowania zgodnie z wykonanymi zmianami).
           1. Kryterium sukcesu otrzymywanie alertów i monitów bezpieczeństwa po wykonanych zmiana dla co najmniej 5 testów.
        3. Monitoring w zakresie SDN Advance Security NG-Firewall / IDS / IPS / URL-Filtering / Malware Protection.
        4. Kryterium sukcesu zachowanie uruchomionych funkcjonalności oprogramowania na etapie A i B.
        5. Katalog usług, automatyzacji, orkiestracji zadań, migracji posiadanych funkcjonalności, wykonanym migracji, integracji i dostosowania do potrzeb Zamawiającego.
           1. Kryterium sukcesu potwierdzenie zakończenia wymaganych migracji zgłoszonych przez Zamawiającego.
           2. Kryterium sukcesu dostępność i funkcjonowanie wymaganych usług w katalogu, procesów automatyzujących i zadań orkiestrowanych.
        6. Integracji z systemami zewnętrznymi m.in. Solarwinds, Zabbix.
  2. Wykonanie Testów Odbiorczych przez Wykonawcę przy udziale Zamawiającego weryfikujących wymagane zmiany i funkcjonalności Chmury dla etapu docelowego.
  3. Uzyskanie akceptacji Zamawiającego dla wyników testów odbiorczych, zgodności z BOM, braku błędów i awarii, nie więcej jak dwie usterki.

### Orkiestracja procesu DR pomiędzy OPD1 i OPD2

Wykonawca posiada obecnie oprogramowanie VMware Site Recovery Manager (SRM), które zapewnia zachowanie ciągłości biznesowej i przywracanie po awarii usług. Realizuje automatyczne odzyskiwanie maszyn wirtualnych (VM) między lokalizacjami fizycznymi OPD1 i OPD2, umożliwiając Zamawiającemu planowanie, testowanie i awaryjne wykonywanie procesów DR odzyskiwania usług w drugiej lokalizacji po awarii lub planowanym procesie DR.

1. Zamawiający posiada aktualnie 250 licencji SRM wykorzystywanych w obszarze MGMT (40 szt.) i PRODUKCJA (210 szt.), ważność licencji posiadanych:
   1. 40 szt. dla WD-MGMT ważne do 22 października 2026 r.
   2. 210 szt. dla WD-PRODUKCJA 20 stycznia 2027 r.
2. Wymagane jest zachowanie funkcjonalności zapewnianej przez oprogramowanie VMware Site Recovery Manager (SRM) w ramach posiadanych licencji i Chmury Prywatnej po dostarczeniu Oprogramowania.
3. Posiadane licencje zapewniają ochronę przez awarią OPD (jednej z dwóch lokalizacji OPD1 lub OPD2) dla usług (biznesowych, zarządzania siecią OSE i Systemu) uruchomionych na zasobach Chmury Prywatnej.
4. Posiadane licencje SRM przez Zmawiającego muszą być możliwe do zastosowania już na etapie A dla zachowania mechanizmów DR.
5. Wymagane jest przedłużenie ważności posiadanych licencji na okres obowiązywania Umowy – serwisu Gwarancyjnego lub dostarczenie licencji równoważnych w zakresie funkcjonalności zgodnych z dostarczonym Oprogramowaniem SDDC (tego samego producenta).

### Wymagania w zakresie funkcjonalności oprogramowania Chmury Prywatnej

Zamawiający posiada zaimplementowaną grupę funkcjonalności wykonanych w ciągu ostatnich 5 lat użytkowania Systemu i są to m.in.

1. Profile ustawień m.in. serwerów HCI w VMware vCenter sprawdzające zgodność konfiguracji z szablonem.
2. Automatyzacje oparte na językach skryptowych odpowiedzialne za monitorowanie, alertowanie, raportowanie m.in. w zakresie bezpieczeństwa, wytycznych.
3. Orkiestracja zadań administracyjnych.
4. Egzekwowanie zdefiniowanych ustawień bezpieczeństwa i standaryzacji.
5. Market place portal samoobsługowy w obszarze usług: maszyn wirtualnych / K8s / Konfiguracji / SDN / Usług wspierających.

Wymagane jest dostosowanie posiadanych funkcjonalności w ramach Oprogramowania SDDC.

Kryterium sukcesu dla zachowania wymaganych funkcjonalności obejmuje zachowanie minimum 80% posiadanych funkcji lub zastąpienie ich tożsamymi realizującymi ten sam cel/efekt funkcjonalny.

### Wymagania w zakresie funkcjonalności monitorowania Chmury Prywatnej

Zamawiający posiada oprogramowanie nadzorujące i monitorujące infrastrukturę i usługi Chmury Prywatnej. Oprogramowanie SDDC musi zapewnić co najmniej:

1. Integracje z posiadanym oprogramowaniem w zakresie monitorowania, raportowania i zbierania metryk.
2. Aktywne monitorowanie z poziomu minimum lokalizacji ODP3, usług uruchomionych w OPD/ROPD, ich dostępności historii i metryk (CPU, RAM, DYSK).
3. Automatyzacje, która musi wykrywać nowe usługi i dodawać je do bazy monitorowania generując metryki m.in. dostępności.
4. Cykliczne raportowanie i monitorowanie zmian w statusie usług, dynamiczne alarmy, raporty.
5. Monitorowanie usług uruchomionych i zagnieżdżonych w sieci SDN w zamkniętych sieciach bez komunikacji na zewnątrz.
6. Monitorowanie zainstalowanych agentów i ich stanu uruchomienia/pracy/dostępności (automatycznego uruchamiania w przypadku wykrycia niedostępności).

### Wymagania w zakresie realizacji Umowy

1. Zamawiający wymaga dostawy licencji/subskrypcji na Oprogramowanie SDDC dla OPD we wskazanych powyżej (pkt. 5) terminach.
2. Wykonawca w okresie Umowy zobowiązany jest wykonywać zadania dodatkowe zlecane w ramach Prac Zleconych opisane w niniejszym dokumencie;
3. Zamawiający wymaga zakończenia realizacji zleconych zadań w ramach Prac Zleconych (Opcji) w terminie wskazanym poniżej w pkt.7; powyższy termin obowiązuje, jeżeli Zamawiający nie ustali innego terminu lub nie wystąpią obiektywne ograniczenia po stronie Zamawiającego lub oprogramowania (wsparcie producenta).
4. Oprogramowanie SDDC dla OPD musi podlegać gwarancji producenta w zakresie obszarów Compute, Storage, Network, Orkiestracji, K8s i narzędzi automatyzacji monitoringu, administracji, katalogu usług, np.: w przypadku oferowania oprogramowania uzupełniającego dodatkowego rozszerzającego wymagane funkcjonalności oferowany producent musi być partnerem technologicznym producenta Oprogramowania SDDC.
5. Prace wdrożeniowe nie mogą zaburzyć działania infrastruktury Chmury Prywatnej jak i uruchomionych usług.
6. Jeżeli do poprawnego działania operacyjnego dostarczanego Oprogramowania Chmury Prywatnej, niezbędne jest wykorzystanie dodatkowych elementów oprogramowania, licencji/subskrypcji (np. związanych z aspektem zarządzania, przełączania, wysokiej dostępności usług w przypadku awarii lub testów), nieujętych wprost w szczegółowym opisie wymagań, należy je przewidzieć i dostarczyć w ramach oferowanej rozbudowy i wynagrodzenia z tytułu realizacji przedmiotu zamówienia;
7. Oferowane Oprogramowanie SDDC musi być produktem rozwijanym z minimum 5 letnią historią wersji, zaoferowana wersja musi być zgodna z aktualnymi Urządzeniami Systemu w najnowszej stabilnej wersji Oprogramowania;
8. Wymagany jest dostęp dla Zamawiającego do materiałów producenta Oprogramowania SDDC, które zostało zaoferowane w ramach Chmury Prywatnej dla OPD, takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe, platforma szkoleniowa w ramach oferowanego Oprogramowania SDDC, laboratoria testowe - pokazowe z funkcjonalności oferowanych w ramach Oprogramowania SDDC;
9. Wymagany jest dostęp dla Zamawiającego do bezpośredniego wsparcia producenta Oprogramowania, które w ramach Umowy objęte jest usługą Gwarancji;
10. W okresie Umowy Zamawiający będzie wspierany przez technicznego asystenta w procesie rozwiązywania problemów, błędów i analizy zmian w stosie technologicznym celem poprawy procesu wymiany informacji i eskalacji zadań priorytetowych pomiędzy producentem, a klientem Oprogramowania.
    1. Wsparcie będzie realizowane w dni robocze
    2. Eskalacja zgłoszonych błędów będzie procesowana natychmiastowo celem rozwiązania w przypadku krytycznych awarii.
    3. Wsparcie obejmuje adaptacje oprogramowania i dostosowanie do potrzeb Zamawiającego.
    4. Asystent będzie posiadał bezpośredni podgląd zgłoszonych wątków u producenta z możliwością eskalacji i procesowania zadań w ramach ich priorytetów.
11. Wymagany jest dostęp dla Zamawiającego do Aktualizacji Oprogramowania objętego Umową;
12. Wymagany jest dostęp do portalu internetowego producenta, umożliwiającego zarządzanie licencjami, zgłoszonymi awariami i przydział uprawień dla współpracujących podmiotów w procesie utrzymania i rozwoju Chmury Prywatnej;
13. Realizowane zadania w ramach Umowy przez Wykonawcę zostaną wykonana z zachodzeniem HA wysokiej dostępność i ciągłość działania Chmury Prywatnej, zadania będą wykonywane w ustalonych godzinach serwisowych z Zamawiającym m.in. nocnych, poza godzinami roboczymi;
14. Dostarczone Oprogramowanie musi znajdować się na oficjalnej stronie producenta w zakresie kompatybilności z posiadanymi serwerami HCI DELL Technologies - Załącznik H1.
15. Wykonawca zobowiązany jest współpracować z Zamawiającym i podmiotami zewnętrznymi odpowiedzialnymi za utrzymanie i rozwój Chmury Prywatnej.
16. Prowadzenie Prac Zleconych nie może zakłócić funkcjonalności Chmury Prywatnej w trakcie realizacji przedmiotu umowy;
17. W trakcie realizacji poszczególnych etapów zmian i Prac Zleconych Wykonawca zobowiązany jest współpracować z innymi podmiotami wyznaczonymi m.in. w trakcie wykonywania rekonfiguracji Systemu w ramach Chmury Prywatnej, proces ten będzie koordynowany przez Zamawiającego zgodnie z ustalonym harmonogramem.

# Wymogi na równoważność dla Oprogramowania SDDC

Poniżej wymieniono szczegółowe wymagania w zakresie równoważności dla Oprogramowania oferowanego w ramach Umowy.

Oprogramowanie zastosowane do rekonfiguracji, zbudowania i użytkowania chmury prywatnej musi być dostarczone z wszystkimi wymaganymi licencjami na okres obowiązywania Umowy. Oprogramowanie musi zapewniać licencje terminowe lub czasowe subskrypcyjne, tj. licencja na określony czas wraz ze wsparciem technicznym do tych licencji świadczonym przez producenta zaoferowanego oprogramowania.

Licencje oferowanego Oprogramowania muszą być dostarczone w formie licencji lub subskrypcji na zasoby serwerów HCI „per procesor” lub „per core” fizyczny rdzeń procesora fizycznego i zasoby dyskowe SDS serwerów HCI.

1. Dostarczone Oprogramowanie musi posiadać wymienione poniżej moduły, pochodzące od jednego producenta oprogramowania celem zachowania spójnego wsparcia technicznego.
2. Wymagane moduły oprogramowania:
   1. Do wirtualizacji mocy obliczeniowej Compute.
   2. Do wirtualizacji przestrzeni dyskowej Storage SDS.
   3. Do tworzenia sieci wirtualnych Network SDN.
   4. Do zarządzania klastrami obliczeniowymi – wirtualizacyjnymi.
   5. Do instalacji i zarządzania modułami chmury prywatnej.
   6. Do monitorowania i zarządzania pojemnością chmury prywatnej.
   7. Do automatyzacji procesów, katalogu usług.
   8. Do zbierania, korelowania i analizowania logowania zdarzeń.
   9. Do tworzenia platformy konteneryzacyjnej opartej na orkiestracji klastrów Kubernetes Cloud Native.
   10. Do monitorowania i analizowania sieci oraz polityk firewall w sieciach wirtualnych SDN Overlay i fizycznych Underlay.
   11. Obsługi portalu samoobsługowego z cyklem życia usług i aplikacji zapewniając automatyczne tworzenie m.in. klastrów K8s, mikro usług, maszyn wirtualnych z bazami danych MySQL i Postres, gotowych aplikacji.
3. W zakresie wirtualizacji mocy obliczeniowej Zamawiający wymaga:
   1. Licencje oferowanego oprogramowania muszą być zaoferowane na wszystkie zasoby obliczeniowe posiadane przez Zamawiającego w ramach załącznika H1 i wymienione dla etapów A, B i C w pkt 5.
   2. Oferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
   3. W oferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 2GB pamięci operacyjnej RAM serwera fizycznego.
   4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w minimum: 256 logicznych wątków, 6TB pamięci fizycznej RAM tego serwera oraz 2 procesorów fizycznych tego serwera.
   5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do minimum 256 procesorów wirtualnych.
   6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do minimum 6 TB pamięci operacyjnej RAM.
   7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do minimum 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
   8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć minimum 4 porty szeregowe, 2 porty równoległe i 10 urządzeń USB
   9. Oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13.
   10. W celu osiągnięcia maksymalnego współczynnika konsolidacji, Oferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione.
   11. W celu oszczędności pamięci RAM i osiągnięcia maksymalnego współczynnika konsolidacji, oprogramowanie musi umożliwiać wykorzystanie dysków NVMe jako dodatkowa pamięć RAM do przechowywania danych typu zimne bloki danych.
   12. Oprogramowanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych.
   13. Oprogramowanie 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”.
   14. Oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi.
   15. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
   16. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
   17. Oferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
   18. Oferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 portów
   19. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych.
   20. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN).).
   21. Oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych minimum 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
   22. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
   23. Oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.
   24. Oprogramowanie, w przypadku musi być zaoferowane z zarządcą klastrów i 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. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut.
       1. Proces przełączania usług musi być realizowany przez narzędzia automatyzujące zadania i realizujące zadanie zgodnie z przygotowanym harmonogramem dla DR.
       2. Oprogramowanie musi umożliwiać wykonywanie testów bez wspływu na działające i chronione zasoby – maszyny wirtualne
       3. Oprogramowanie realizujące proces odzyskania (VM) maszyn wirtualnych w lokalizacji pozostałej po awarii musi umożliwiać odzyskanie wcześniejszej repliki VM niż ostatniej jeżeli chroniona maszyna posiadała kilka replik historycznych.
   25. Oferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
   26. Oferowane oprogramowanie, działające pod zarządcą klastrów, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi.
   27. Oferowane oprogramowanie, dla środowisk klastrowych musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. High Availability).
   28. Oferowane oprogramowanie, działające klastrowym w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji proces musi być automatyczny wspomagając proces aktualizacji klastrów obliczeniowych.
   29. Oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
   30. Oferowane oprogramowanie, działające pod zarządcą klastra, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (z minimum dwoma procesorami wirtualnymi), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną.
   31. Oferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 60 TB.
   32. Oferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
   33. Producent oferowanego oprogramowania do wirtualizacji musi oferować rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software Defined Network) jako spójne rozwiązanie SDDC.
   34. Oferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.
   35. Oferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest oferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie.
   36. Wirtualizator w oferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 11, Microsoft Windows Server 2019 oraz Microsoft Windows Server 2022.
   37. Oferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.
   38. Oferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 11 oraz Microsoft Windows 2022. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 11 lub Microsoft Windows Server 2019 oraz Microsoft Windows Server 2022 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
   39. Oferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
   40. Oferowane oprogramowanie, działające pod zarządcą klastra, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych i nie wspieranych wersjach. Taka funkcjonalność powinna być dostępna dla minimum trzech producentów serwerów obecnych na rynku urządzeń HCI.
   41. Oferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
   42. Oferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
   43. Oferowane oprogramowanie, działające pod zarządcą klastra, 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.
   44. Oferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany.
   45. Oferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.
   46. Oferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi być uruchamiana w pamięci operacyjnej wirtualizatora.
   47. Oferowane oprogramowanie, działające pod zarządcą klastra, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego.
   48. Oferowane oprogramowanie podczas pracy w klastrze zarządzanym musi umożliwiać automatyczne równoważenie obciążenia CPU/MEMORY serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
   49. Oferowane oprogramowanie musi posiadać certyfikację dla pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji AI i frameworków przeznaczonych dla kompleksowego rozwiązania AI.
   50. Oferowane oprogramowanie musi umożliwiać włączenie najnowszej generacji procesorów graficznych NVIDIA z 2025 roku do swojego środowiska wirtualnego i skorzystanie z takich funkcji jak Multi-Instance GPU (MIG), pozwalające na współdzielenie cykli GPU przez wielu użytkowników.
       1. Zgodność z posiadaną kartą A100 NVIDIA
   51. Oferowane oprogramowanie do wirtualizacji, działające pod zarządcą klastra, musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (Hypervisora), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
   52. Oferowane oprogramowanie, działające pod zarządcą klastra, musi umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne istniejące w tym klastrze. 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. Przełącznik rozproszony musi współpracować z protokołem NetFlow lub IPFIX.
   53. Zaimplementowany w oferowanym oprogramowaniu przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port celem analizy ruchu sieciowego.
   54. Zaimplementowany w oferowanym oprogramowaniu przełącznik rozproszony 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. Oferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych
   56. Oferowane oprogramowanie, działające pod zarządcą klastra, 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 historyczne
   57. Oferowane oprogramowanie, działające pod zarządcą klastra, 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 wirtualnymi.
   58. Oferowane oprogramowanie, działające pod zarządcą klastra, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (minimum ośmiu procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
   59. Oferowane oprogramowanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
   60. Oferowane oprogramowanie, działające pod zarządcą klastra, musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
   61. Oferowane oprogramowanie musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych m.in. GPU.
   62. Oferowane oprogramowanie, działające pod zarządcą klastra 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
   63. Oferowane oprogramowanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU zainstalowanego w serwerze fizycznym do maszyn wirtualnych
   64. Oferowane oprogramowanie musi wspierać funkcjonalność trwałej, nieulotnej pamięci (ang. Persistent Memory)
   65. Oferowane oprogramowanie musi wspierać protokół Remote Direct Memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2 i iSCSI rozszerzenie dla RDMA (iSER). Wymaga się, aby maszyny wirtualne można było konfigurować z wykorzystaniem protokołu RDMA
   66. Oferowane oprogramowanie musi posiadać możliwość testowania wybranych serwerów (w szczególności tych, na których uruchomione są aplikacje przetwarzające dane wrażliwe i które mają dostęp do kluczy szyfrujących maszyny wirtualne) w celu weryfikacji, czy oprogramowanie jest autentyczne i nie zostało zmodyfikowane. Funkcjonalność ta powinna działać w oparciu o chip TPM 2.0 zainstalowany w serwerze i powinna odbywać się poza centralną konsolą zarządzającą (która sama jest maszyną wirtualną) wyłącznie w oparciu o sprzętowe źródło zaufania (hardware root of trust). Tylko serwery, które przejdą weryfikację mogą mieć dostęp do kluczy szyfrujących
   67. W przypadku pracy w oparciu o zarządzanie z centralnej konsoli zarządzającej, centralna konsola zarządzająca musi wspierać możliwość wcześniejszego i automatycznego przetestowania wpływu jej aktualizacji na pozostałe podłączone do niej komponenty klastra oraz uruchomione na nim funkcjonalności. Musi również wspierać proces aktualizacji całego klastra poprzez automatyczne raportowanie kolejności aktualizacji podłączonych do niej komponentów i rekomendowanej ich wersji.
   68. Oferowane oprogramowanie musi wspierać możliwość eksportu konfiguracji centralnej konsoli zarządzającej wirtualizacją przez API i umożliwiać wykorzystanie jej jako szablonu przy kreowaniu kolejnych instancji centralnej konsoli zarządzającej oraz do weryfikacji poprawności konfiguracji zainstalowanych już instancji.
   69. Oferowane oprogramowanie musi wspierać funkcje DPU (ang. Digital Processing Unit) na zasadzie przekazywania obciążeń sieci wirtualnej z hipervisora do oddzielnej jednostki DPU zainstalowanej w serwerze fizycznym.
   70. Oferowane oprogramowanie musi wspierać funkcjonalność bezpośredniego tworzenia kontenerów oraz klastrów Kubernetes na hiperwizorze (warstwie wirtualizatora) za pomocą dostarczonej konsoli zarządzającej i orkiestracji Kubernetes (Kubectl).
4. W zakresie zarządzania klastrami wirtualizacyjnymi Zamawiający wymaga:
   1. Oprogramowanie do zarządzania klastrami wirtualizacyjnym musi obejmować fizyczne core procesora urządzeń HCI.
   2. Oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się, aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtual appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych musi stanowić jednolity produkt, którego ustawienia i bieżący stan musi być możliwy do eksportu cyklicznego.
   3. Oferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów.
   4. Oferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
   5. Oferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5.
   6. Oferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się, aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz http.
   7. Oferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage)
   8. Oferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5
   9. Oferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
   10. Oferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
   11. Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości minimum 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
   12. Oferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
   13. Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielanie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
5. W zakresie konsoli/oprogramowania do instalacji i zarządzania komponentami chmury prywatnej Zamawiający wymaga:
   1. Oferowane oprogramowanie musi posiadać konsole centralną do automatycznej instalacji i/lub konfiguracji oprogramowania do wirtualizacji serwerów fizycznych, macierzy dyskowej typu SDS (ang. Software Defined Storage) na serwerach, wirtualizacji sieci typu SDN (ang. Software Defined Network) wraz z mechanizmami bezpieczeństwa. Dodatkowo oprogramowanie, z tej samej konsoli, musi być w stanie aktualizować wszystkie powyższe komponenty oprogramowania.
   2. Oferowane oprogramowanie musi posiadać narzędzia automatyzujące i upraszczające proces wdrażania stosu oprogramowania infrastrukturalnego do wirtualizacji serwerów x86, wirtualizacji sieci oraz tworzenia macierzy dyskowej typu SDS poprzez zautomatyzowaną instalację oprogramowania, tworzenie klastrów obliczeniowych (w tym klastry obliczeniowe pod środowiska typu VDI, klastry Kubernetes) oraz dedykowanego klastra zarządzającego całością zainstalowanej za pomocą przedmiotowego oprogramowania chmury prywatnej.
   3. Oferowane oprogramowanie musi posiadać mechanizmy aktualizacji całego stosu zainstalowanego w oparciu o niego oprogramowania wirtualizującego oraz definiowania harmonogramu i zakresu tych aktualizacji
   4. Mechanizmy aktualizacji zawarte w zaoferowanym oprogramowaniu muszą umożliwiać korzystanie z aktualizacji w dwóch trybach – przy podłączaniu do portalu z poprawkami i w trybie offline – czyli możliwość wcześniejszego wgrania poprawek do repozytorium.
   5. Oferowane oprogramowanie musi posiadać, na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerów sprzętowych. Wymagane jest wsparcie dla min. 3 niezależnych producentów sprzętu serwerowego
   6. Oferowane oprogramowanie musi być w stanie instalować automatycznie i aktualizować komponenty środowiska wirtualnego, minimum: wirtualizacja mocy obliczeniowej, wirtualizacja przestrzeni dyskowej, wirtualizacja sieci komputerowej, moduł zarządzana i optymalizacji pojemności, moduł gromadzenia logów z infrastruktury
   7. Oferowane oprogramowanie musi posiadać, na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerów sprzętowych. Wymagane jest wsparcie dla min. 3 niezależnych producentów sprzętu serwerowego x86
   8. Oferowane oprogramowanie musi wspierać funkcjonalność zarządzania hasłami dla komponentów, minimum takich jak: wirtualizacja mocy obliczeniowej, wirtualizacja przestrzeni dyskowej, wirtualizacja sieci komputerowej.
   9. Oferowane oprogramowanie musi dostarczyć co najmniej 3 metody zmiany haseł na przykład: automatyczne generowanie haseł, zmiana na własne hasło i możliwość podłączania managera haseł poprzez API.
   10. Oferowane oprogramowanie musi zapewniać autorotację haseł.
   11. Oferowane oprogramowanie musi umożliwiać zarządzanie certyfikatami SSL z konsoli centralnej dla całego stosu zainstalowanego w oparciu o niego oprogramowania wirtualizującego.
   12. Oferowane oprogramowanie musi zapewniać możliwość wykonywania kopii zapasowych konfiguracji całego stosu zainstalowanego w oparciu o niego oprogramowania wirtualizującego oraz definiowania harmonogramu wykonywania kopii zapasowych
   13. Oferowane oprogramowanie musi zapewniać integrację i automatyzację warstwy oprogramowania monitorującego i zbierającego logi poprzez kontrolę aktualizacji.
6. W zakresie monitorowania i zarządzania pojemnością chmury prywatnej Zamawiający wymaga:
   1. Licencje zaoferowanego oprogramowania muszą być równe liczbie zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.
   2. Oferowane oprogramowanie musi uzyskiwać informacje na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością
   3. Oferowane oprogramowanie musi za pomocą wbudowanych inteligentnych algorytmów przewidywać trendy związane z pojemnością środowiska wirtualnego opartego na klastrach HCI.
   4. Oferowane oprogramowanie musi posiadać funkcjonalność dającą możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, zasoby dyskowe)
   5. Oferowane oprogramowanie musi mieć możliwość tworzenia unikalnego zbioru obiektów korespondujących funkcjami z obiektami Datacenter, tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem.
   6. Oferowane oprogramowanie musi mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów z Data Center w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.
   7. Oferowane oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy predykcyjnego obliczania pojemności na zasadzie: "co jeśli" dla minimum: co jeśli dodamy kolejne maszyn wirtualne. Rozwiązanie będzie umożliwiało definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności musi odnosić się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia.
   8. Oferowane oprogramowanie musi mieć funkcjonalność zapisywania i przechowywania różnych scenariuszy "co by było, gdyby" w obszarze zarządzania pojemnością. Zapisane scenariusze muszą wpływać na prognozowanie analizy pojemności
   9. Oferowane oprogramowanie musi w obszarze zarządzania pojemnością mieć funkcjonalność definiowania poziomu konsolidacji/wirtualizacji (ilość wirtualnych rdzeni do fizycznych lub ilość wirtualnej pamięci do fizycznej) po to, aby w zakresie poprawnie wykonywać predykcję pojemności w przyszłości w modelu przypisanych zasobów wirtualnych (ilość wirtualnych rdzeni do fizycznych lub ilość wirtualnej pamięci do fizycznej)
   10. Oferowane oprogramowanie musi monitorować infrastrukturę HCI Zamawiającego opartą o dostarczone oprogramowanie compute, storage, network.
   11. Zaoferowane oprogramowanie, w obrębie monitorowania, będzie posiadało rozwiązanie generowania alertów na podstawie korelacji wykrytych w środowisku wirtualnym anomalii i symptomów, a nie pojedynczych monitorowanych metryk.
   12. Oferowane oprogramowanie musi posiadać funkcjonalność dostarczania informacji na temat rekomendowanych przez producenta zmian, mających na celu prawidłowe działanie środowiska SDDC m.in. analiza podatności.
   13. Oferowane oprogramowanie musi posiadać wbudowane komponenty integracyjne obsługujące zewnętrzne kolektory logów i zdarzeń.
   14. Oferowane oprogramowanie musi posiadać funkcjonalność monitorowania i alertowania na temat zgodności serwerów HCI z najlepszymi praktykami bezpieczeństwa dla zaoferowanego oprogramowania w zakresie „hardening" oraz DISA (Defence Information Systems Agency), FISMA (Federal Information Security Management Act), ISO, CIS (Center of Internet Security), PCI (Payment Card Industry) i HIPAA (Health Insurance Portability and Accountability Act).
   15. Oferowane oprogramowanie musi posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem zwirtualizowanym.
   16. Oferowane oprogramowanie musi wizualizować w trybie online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down” do minimum 2 poziomów zagnieżdżenia.
   17. Oferowane oprogramowanie musi posiadać funkcjonalność graficznej prezentacji wyników (ang. dashboard).
   18. Oferowane oprogramowanie musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich dodatkowego wytwarzania podczas używania oprogramowania..
   19. Oferowane oprogramowanie musi dokonywać automatycznej predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych (wbudowanego w zaoferowane oprogramowanie) oraz planów uruchomienia kolejnych serwerów wirtualnych. Zakres historii do analityki predykcyjnej musi wynosić minimum 6 miesięcy.
   20. Oferowane oprogramowanie musi umożliwiać przeglądanie linii trendu monitorowanych parametrów.
   21. Oferowane oprogramowanie musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń wirtualnych jak i fizycznych, związanych z wirtualizatorem opartym o rozwiązanie Compute, SDS oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym.
   22. Oferowane oprogramowanie musi umożliwiać monitorowanie środowisk w czasie rzeczywistym (przeglądane informacje powinny ukazywać się w trybie rzeczywistym – dopuszczane jest maksymalne opóźnienie nie większe niż 5 minut).
   23. Oferowane oprogramowanie musi pozyskiwać oraz prezentować, w formie wykresów oraz tabelaryczno-tekstowej, zbiorczo oraz osobno, dla każdego systemu operacyjnego, aktualne i historyczne dane dotyczące utylizacji CPU, RAM, zasobów dyskowych oraz interfejsów sieciowych.
   24. Oferowane oprogramowanie musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów. Stopień szczegółowości zapisywania metryk musi wynosić co najmniej 5 punktów danych na minutę w ciągu 5 lat.
   25. Oferowane oprogramowanie musi umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, zasoby dyskowe).
   26. Oferowane oprogramowanie musi umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł.
   27. Oferowane oprogramowanie musi posiadać możliwość kasowania, wykonywania kopii migawkowych (ang. snapshot), włączania oraz wyłączania maszyn wirtualnych posadowionych na monitorowanym środowisku wirtualnym.
   28. Oferowane oprogramowanie musi automatycznie przeszukiwać i analizować zebrane dane w celu wynajdywania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, RAM, HDD) w monitorowanym środowisku.
   29. Oferowane oprogramowanie musi posiadać funkcjonalność automatycznego alarmowania w sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o minimum nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej).
   30. Oferowane oprogramowanie musi posiadać możliwość dowolnego przypisywania powiadamiania o alertach w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie przez użytkownika).
   31. Oferowane oprogramowanie musi pozwalać na odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z powiązanymi z nimi poradami eksperckim.
   32. Oferowane oprogramowanie musi umożliwiać definiowanie alertów związanych z: zarządzaniem pojemnością, zarządzaniem wydajnością, anomaliami w środowisku, zarządzaniu dostępnością dla monitorowanego środowiska.
   33. Oferowane oprogramowanie musi mieć posiadać funkcjonalność przypisania alertu do administratora/operatora rozwiązującego problem.
   34. Oferowane oprogramowanie musi integrować się z produktem odpowiedzialnych za analizę logów (poprzez integracje Zamawiający rozumie możliwość przesyłania danych z rozwiązania odpowiedzialnego za logi do zaoferowanego oprogramowania).
   35. Oferowane oprogramowanie musi mieć możliwość generowania gotowych, predefiniowanych raportów o stanie środowiska monitorowanego.
   36. Oferowane oprogramowanie musi integrować się z produktem odpowiedzialnych za analizę sieci (przez integrację Zamawiający rozumie możliwość dostarczania danych o wykrywaniu aplikacji z rozwiązania odpowiedzialnych za sieć do oferowanego oprogramowania).
   37. Oferowane oprogramowanie musi posiadać funkcjonalność gotowego pulpitu kierowniczego (ang. dashboard) za pomocą którego administrator będzie posiadał gotowe trzy kolumny z następującymi informacjami:
       1. Zdarzenia jakie wystąpiły w zadanym okresiedla analizowanego problemu, min. dla: wirtualnych maszyn, sieci wirtualnej, wirtualnej przestrzeni dyskowej
       2. Anomalie, jakie wystąpiły w zadanym okresiedla analizowanego problemu
       3. Zmiany w konfiguracji monitorowanej infrastruktury jakie wystąpiły w zadanym okresie dla analizowanego problemu
       4. Analiza danych ukazująca powyższe wyniki prezentowane w dashboard musi odbywać się automatycznie poprzez mechanizmy uczenia się maszynowego zaoferowanego oprogramowania do monitorowania na podstawie zakresu czasowego definiowanego przez użytkownika tego dashborad. Dodatkowo użytkownik musi mieć możliwość definiowania, dla którego obiektu, np. wybranej maszyny wirtualnej należy przeprowadzić analizę, a następnie wyświetlić jej wyniki.
   38. Oferowane oprogramowanie musi wspierać zbieranie minimum 0,4 mln obiektów na klaster minimum 40 mln metryk; ilość obsługiwanych jednoczesnych wywołań Rest API do pobierania danych wynosi minimum 3000.
   39. Oferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów umożliwiających integrację z systemami firm trzecich monitorującymi infrastrukturę np. IPAM.
   40. Oferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych paczek monitorujących dla rozwiązań firm trzecich.
   41. Oferowane oprogramowanie musi umożliwiać konfigurację trybu wysokiej dostępności (ang. HA) dla każdego swojego komponentu w celu uniknięcia awarii pojedynczego elementu. Należy zapewnić architekturę, która zapobiega utracie danych w przypadku awarii jednego z węzłów klastra.
   42. Oferowane oprogramowanie musi posiadać funkcjonalność zmiany parametrów maszyn wirtualnych, minimum CPU i RAM, za pomocą wygenerowanego w tym oprogramowaniu zadania. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie w/w zadania, po wygenerowaniu (zadanie może być uruchamiane w momencie utworzenia lub w dowolnie skonfigurowanym przez użytkownika czasie).
   43. Oferowane oprogramowanie musi posiadać możliwość zastosowania dodatkowych adapterów odpowiadających za monitorowanie systemów zewnętrznych takich jak m.in: macierze dyskowe, chmury obliczeniowe, serwery fizyczne, przełączniki LAN/SAN, umożliwiając tym samym wykorzystanie dedykowanych dodatkowych mechanizmów monitorujących określone komponenty.
   44. Oferowane oprogramowanie musi umożliwiać elastyczne dostosowanie wyglądu interfejsu użytkownika w zależności od indywidualnych potrzeb.
   45. Oferowane oprogramowanie musi zapewniać kompleksowe możliwości wyszukiwania po wszystkich przechowywanych obiektach, ich właściwościach i wartościach metryk.
   46. Oferowane oprogramowanie musi posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk.
   47. Oferowane oprogramowanie musi posiadać funkcję tzw. konfiguratora własnych pulpitów kierowniczych (ang. dashboard) na podstawie zgromadzonych danych w rozwiązaniu. Za pomocą tej funkcjonalności rozwiązanie musi umożliwiać tworzenie zaawansowanych pulpitów kierowniczych (dashborad).
   48. Oferowane oprogramowanie musi posiadać funkcjonalność monitorowania systemów operacyjnych serwerów wirtualnych opartych uruchomionych w wirtualizatorze Compute (w tym Windows, Linux) i dostarczać takich danych jak: zużycie pamięci, nazwa DNS, wykorzystanie systemu plików.
   49. Oferowane oprogramowanie musi posiadać funkcjonalność wykrywania usług (Service Discovery) serwerów wirtualnych opartych na wirtualizatorze Compute (w tym Windows, Linux) bez agentów. Administrator może wybrać pożądaną usługę z biblioteki lub określić własną.
   50. Oferowane oprogramowanie musi posiadać funkcjonalność monitorowania systemów operacyjnych (m.in. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym.
   51. Oferowane oprogramowanie musi posiadać funkcjonalność integracji z rozwiązaniami ServiceNow oraz do Automatyzacji.
   52. Oferowane oprogramowanie musi posiadać gotowe paczki do monitorowania (ang. management packs) dla produktów SDDC, Automatyzacji
   53. Oferowane oprogramowanie musi mieć funkcjonalność tworzenia scenariuszy pojemnościowych na zasadzie: "co jeśli" dla minimum: CPU, RAM oraz przestrzeni dyskowej dla następujących elementów:
       1. Dodawania nowych serwerów fizycznych.
       2. Dodawania dodatkowych elementów SDS..
       3. Migracji do AWS, Azure, Google Cloud.
   54. Oferowane oprogramowanie musi posiadać możliwość matematycznego wyliczania wartości super metryki na podstawie innych, gromadzonych i monitorowanych metryk podstawowych. Super metryka to formuła matematyczna, która zawiera jedną lub więcej metryk. Jest to niestandardowa metryka, którą można zaprojektować w rozwiązaniu, aby pomóc śledzić kombinacje metryk, z jednego obiektu lub z wielu obiektów.
   55. Oferowane oprogramowanie musi wykrywać usługi uruchomione na monitorowanych maszynach wirtualnych, a następnie budować relacje lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacja sieciowej.
   56. Oferowane oprogramowanie musi posiadać możliwość, po uruchomieniu alarmu, wykonywać na podstawie tego alarmu, automatyczne działania dotyczących akcji naprawczych.
   57. Oferowane oprogramowanie musi posiadać funkcjonalność monitorowania urządzeń firm trzecich typu macierze dyskowe, urządzenia sieciowe, a także wirtualizatorów innych niż rozwiązanie dostarczone za pomocą specjalnie przygotowywanych paczek do monitorowania
   58. Oferowane oprogramowanie musi umożliwiać wykazanie zrównoważonego rozwoju (sustainability) w centrach danych klienta poprzez pokazanie redukcji śladu węglowego wynikającej z wdrożenia wirtualizacji serwerów, optymalizacji obciążeń i innych działań mające na celu oszczędności.
   59. Oferowane oprogramowanie musi posiadać funkcjonalność monitorowania aplikacji, serwerów aplikacyjnych oraz baz danych firm trzecich za pomocą specjalnie przygotowywanych paczek (ang. management packs) firm trzecich lub producenta oferowanego oprogramowania.
   60. Oferowane oprogramowanie musi mieć możliwość monitorowania zmian na poziomie systemów operacyjnych w tym konfiguracji tych systemów.
   61. Oferowane oprogramowanie musi mieć gotowe paczki (ang. management packs) do monitorowania platform typu Multi-Cloud, tj. AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform i rozwiązań kontenerowych Kubernetes.
   62. Oferowane oprogramowanie musi posiadać gotową do użycia funkcjonalność (Out-of-the-Box dostępną po zainstalowaniu oprogramowania) w zakresie wykrywania, monitorowania i rozwiązywania problemów dla aplikacji firm trzecich w postaci gotowych do użycia bibliotek Dashboardów, Alertów i Raportów.
   63. Zamawiający wymaga, aby w ramach oprogramowania do monitoringu można było uruchamiać w nim dedykowane wtyczki przygotowywane przy pomocy narzędzia dostarczonego przez producenta w ramach przedmiotowego postępowania.
7. W zakresie automatyzacji Zamawiający wymaga:
   1. Oferowane oprogramowanie musi posiadać portal typu „Self-Service” do automatycznego tworzenia i uruchamiania wirtualnych systemów operacyjnych, platform aplikacyjnych i całych zestawów/systemów maszyn wirtualnych.
   2. Interfejs graficzny UI (ang. user interface) musi być dostępny poprzez przeglądarkę internetową, wspierać technologię opartą o HTML5 oraz posiadać możliwość katalogowania widoku poszczególnych typów usług według własnego wzorca.
   3. Oferowane oprogramowanie musi posiadać możliwość modyfikacji właściwości obiektów w katalogu (w tym w szczególności konfiguracji wirtualnego sprzętu: CPU, RAM, storage, network), zarówno przed provisioningiem usługi jak i po provisioningu
   4. Zaoferowane oprogramowanie, za pomocą dodatkowej integracji, musi oferować w ramach katalogu usług informacje o kosztach danej usługi - modyfikowana na bieżąco w zależności od konfiguracji wirtualnego sprzętu (np. ilość instancji, ilość pamięci RAM, ilość CPU)
   5. Oferowane oprogramowanie musi prezentować informacje w postaci wykresów o kluczowych metrykach maszyny wirtualnej, wytworzonej w ramach ustalonego procesu takich jak CPU, pamięć, IOPS, sieć
   6. Oferowane oprogramowanie musi umożliwiać modyfikację wirtualnego sprzętu przypisanego do obiektu po "provisioningu" danego obiektu z katalogu. Musi pozwalać na rozszerzalność akcji/działań dla dostarczonych zasobów, np. włączanie/wyłączanie maszyn wirtualnych, wykonywanie kopii zapasowych/przywracanie danych maszyn wirtualnych, instalowanie aplikacji, itp.
   7. Oferowane oprogramowanie musi posiadać zestaw wbudowanych procesów/czynności automatyzacji dostarczania usług wraz z możliwością ich edycji, zmiany konfiguracji i tworzenia nowych „kroków” w procesie cyklu życia konkretnej usługi
   8. Oferowane oprogramowanie musi informować o statusie usługi w czasie rzeczywistym min: usługa zaakceptowana, zakolejkowana, odrzucona, w trakcie akceptacji. Dodatkowo Oferowane oprogramowanie musi mieć możliwość wysłania informacji poprzez pocztę elektroniczną o zmianie statusu usługi
   9. Oferowane oprogramowanie musi posiadać możliwość definiowania sieci wirtualnych, które łączą maszyny wirtualne w ramach zarządzanej platformy (w każdym z Data Center będącym elementem projektu) – rozwiązanie musi wspierać natywnie dostarczone rozwiązania SDN .
   10. Oferowane oprogramowanie musi posiadać możliwość definiowania sieci wewnętrznych jak i sieci zewnętrznych połączonych do sieci fizycznej - pozwalającej na komunikację np. do Internetu za pomocą np. NAT – rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN
   11. Oferowane oprogramowanie musi posiadać możliwość definiowania fizycznych zasobów (mocy obliczeniowej) oraz zmiany ich wielkości poprzez powiększenie lub pomniejszenie obiektu) bez wpływu na działanie usług - tj. Obiekt musi być dostępny podczas dokonywanych operacji.
   12. Oferowane oprogramowanie musi posiadać możliwość definiowania logicznych obiektów zawierających wiele wirtualnych elementów w tym wiele maszyn wirtualnych powiązanych ze sobą zależnościami, tak aby w rezultacie administrator systemu mógł stworzyć wielowarstwowy serwis (np. aplikacja CRM (Load Balansowany Web Front-End, Middelware oraz sklastrowany Back End- Baza Danych)
   13. Za pomocą zaoferowanego oprogramowania, administrator musi posiadać możliwość wyboru, które obiekty z katalogu mogą ulegać modyfikacji przez użytkownika końcowego. Wymaga się aby lista obiektów była nie mniejsza niż: liczba wirtualnych procesorów, wielkość pamięci operacyjnej, ilość i wielkość dysków oraz typ wolumenu, ilość kart sieciowych i typy sieci, czas dzierżawy, polityka archiwizacji, hasło administracyjne systemu operacyjnego) przy czym zmiana parametrów przez użytkownika może wymagać dodatkowych akceptacji przy procesie uruchomienia serwisu.
   14. Oferowane oprogramowanie musi posiadać wsparcie dla dostarczonego oprogramowania.
   15. Oferowane oprogramowanie musi posiadać wsparcie dla realizacji modelu: "Projektuj usługę raz, wdrażaj gdziekolwiek".
   16. Oferowane oprogramowanie musi umożliwiać rezerwację zasobów fizycznych dla wybranych grup użytkowników oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników.
   17. Oferowane oprogramowanie musi mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych, określania dla nich zasobów fizycznych, grup użytkowników, wzorców usług a także procesów tworzenia, zarządzania cyklem życia usług.
   18. Oferowane oprogramowanie musi się integrować z innymi systemami zewnętrznymi typu: CMDB, DNS, IPAM, Load Balancer, Service Desk, Monitoring jako pluginy lub napisanych od początku w języku programowania. Efektem powyższej integracji musi być w pełni automatyczny proces tworzenia i zarządzania usługą niewymagający czynności ręcznych.
   19. Oferowane oprogramowanie musi umożliwiać tworzenie nowych abstraktów usług wraz z określeniem ilości i rodzaju zasobów dostępnych dla danej usługi zarówno na etapie tworzenia jak i późniejszej rekonfiguracji danej usługi.
   20. Oferowane oprogramowanie musi umożliwiać obsługiwać języki programowania Python, JavaScript, PowerShell, bash oraz musi zawierać bibliotekę powszechnie używanych komponentów i wspierać pracę z protokołami takimi jak REST, SQL, JDBC, AMPQ, SNMP, AD, SOAP, Email, SSH, PowerCLI.
   21. Oferowane oprogramowanie musi posiadać jedno narzędzie do projektowania usługi opartej na OS, aplikacjach, usług sieciowych tj.: Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa w locie podczas provisioningu - w sieciowym aspekcie rozwiązanie musi mieć wsparcie dla mikrosegmentacji tj. filtrowania ruchu pomiędzy dowolnymi maszynami wirtualnymi również w obrębie tej samej sieci - rozwiązanie musi wspierać natywnie dostarczone rozwiązanie SDN.
   22. Oferowane oprogramowanie musi umożliwiać zbudowanie zunifikowanego Katalogu Usług dla aplikacji, infrastruktury i danych.
   23. Oferowane oprogramowanie musi posiadać interfejs typu „drag-drop” przeznaczony do tworzenia dowolnej aplikacji na podstawie utworzonych wcześniej komponentów, aplikacji, systemów, sieci i polityk bezpieczeństwa oraz innych skryptów pomocnych w automatyzacji.
   24. Oferowane oprogramowanie musi umożliwiać graficzną edycję przebiegu procesu realizacji usług, definiowanie poszczególnych kroków oraz ich danych wejściowych i wyjściowych. Przebiegi procesów mogą być sekwencyjne lub składać się z wielu sekwencji zadań realizowanych równocześnie, musi istnieć możliwość testowania zdefiniowanych procesów realizacji usług przy użyciu debugger-a, który pozwala analizować postęp procesu krok po kroku ze śledzeniem przekazywanych danych.
   25. Oferowane oprogramowanie musi umożliwiać export/import zdefiniowanych procesów realizacji usług do/z pliku w celu przeniesienia definicji pomiędzy różnymi środowiskami i wspierać podejście Infrastructure as Code (IaC). Dodatkowo narzędzie projektowe musi wspierać wdrażanie usług za pomocą kodu Terraform lub Salt.
   26. Oferowane oprogramowanie musi umożliwiać integrację z Active Directory oraz Open LDAP, i wieloma ich domenami w tym samym czasie.
   27. W zaoferowanym oprogramowaniu użytkownik REQUESTER musi mieć możliwość wykonywania wszystkich operacji na swojej usłudze z jednej konsoli tj. Self-Service portalu, bez konieczności posługiwania się innymi narzędziami administracyjnymi.
   28. Oferowane oprogramowanie musi posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli, opartego na rolach: np.: Tenant Admin, Service Architect, Network Architect, Application Architect.
   29. Oferowane oprogramowanie służące do automatyzacji musi standaryzować wdrażanie usług IT oraz eliminować w ten sposób błędy czynnika ludzkiego.
   30. Oferowane oprogramowanie musi dostarczać mechanizmy monitorowania statusu zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług, za pomocą min. portalu Self-Service i powiadomień e-mail.
   31. Oferowane oprogramowanie musi mieć możliwość zgłaszania przez Administratora potrzeby odzyskania poszczególnych zasobów od użytkowników w przypadku ich niewłaściwego wykorzystywania.
   32. Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. Rest API oraz posiadać wbudowaną możliwość integracji Terraform.
   33. Oferowane oprogramowanie musi udostępniać zewnętrzny sklep (marketplace) z opublikowanymi gotowymi do użycia szablonami i usługami.
   34. Oferowane oprogramowanie musi mieć możliwość być skonfigurowane redundantnie, czyli awaria jednego z komponentów, nie może wpływać na świadczenie usług.
   35. Oferowane oprogramowanie musi posiadać wsparcie dla tworzenia (provisioningu) dla dostawców chmury publicznej takich jak: AWS, Microsoft Azure, GCP.
   36. Oferowane oprogramowanie musi posiadać funkcjonalność Platform as a Service, czyli wdrażanie połączonego IaaS z instalacją i zależnościami aplikacyjnymi (również aplikacje w modelu wielowarstwowym).
   37. XaaS (Wszystko jako Usługa) - pełna integracja z systemami zewnętrznymi IT i możliwość wykonywania na nich zdalnie zadań niezbędnych do dostarczenia kompleksowej usługi IT. Minimalne poziomy integracji z zewnętrznymi systemami to: proces zatrudnienia nowego pracownika, założenie/skasowanie skrzynki/skrzynek pocztowych, przestrzeń dyskowa jako usługa, usługi sieciowe, wykonywanie kopii zapasowych i odzyskiwanie usług, zadania związane z Active Directory, instalacja oprogramowania, zarządzanie hasłami.
   38. Oferowane oprogramowanie musi umożliwiać projektowanie ciągłego wdrażania infrastruktury (z ang. Continuous Deployment) i integrować się z narzędziami do tworzenia ciągów wdrożeniowych firm trzecich, takimi jak Jenkins, Artifactory, Git, Jira lub Microsoft TFS.
   39. Oferowane oprogramowanie musi umożliwiać wykonywanie skryptów PowerShell, cmd i innych interpreterów (np. bash) na każdym etapie ciągów wdrożeniowych (również w maszynach wirtualnych).
   40. Oferowane oprogramowanie musi posiadać integrację z oprogramowaniem Ansible Tower w wersji komercyjnej, poprzez gotowe rozszerzenie firmy zewnętrznej – funkcjonalność rozszerzenia musi obejmować co najmniej wykorzystanie obiektów z Ansible Tower w wersji komercyjnej w ramach tworzenia szablonu usługi w rozwiązaniu, jak również operacje dnia drugiego takie jak rejestracja lub wygaszenie aplikacji.
   41. Oferowane oprogramowanie musi umożliwiać integrację z kontenerami tworzonymi w obrębie systemów operacyjnych, np. Linux w celu automatycznej ich instalacji oraz konfiguracji.
   42. Oferowane oprogramowanie musi umożliwiać natywną integrację z dostarczoną platformą orkiestracji Kubernetes Cloud Native.
   43. Oferowane oprogramowanie musi umożliwiać tworzenie/wdrażanie klastrów Kubernetes na platformie Compute z wymaganą konfiguracją w formacie YAML.
8. W zakresie zbierania, korelowania i analizowania logowania logów ze zdarzeń Zamawiający wymaga:
   1. Licencje zaoferowanego oprogramowania muszą być równe liczbie zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.
   2. Oferowane oprogramowanie musi zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń fizycznych wykorzystujących technologię „Syslog
   3. Oferowane oprogramowanie musi integrować się z wymaganym w przedmiotowym postępowaniu oprogramowaniem do monitorowania w ten sposób, że z poziomu konsoli użytkownika oprogramowania do monitorowania musi istnieć możliwość uzyskania natychmiastowego dostępu do logów konkretnego urządzenia fizycznego.
   4. Oferowane oprogramowanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów minimum: liniowych, kołowych i słupkowych.
   5. Oferowane oprogramowanie musi w pełni integrować się z zaoferowanym oprogramowaniem do zarządzania klastrem wirtualizacyjnym.
   6. Oferowane oprogramowanie musi posiadać wbudowaną bazę wiedzy dotycząca logów oraz zdarzeń dla platformy wirtualizacyjnej Vmware.
   7. Oferowane oprogramowanie musi posiadać możliwość udostępniania raportów za pomocą URL kierującego do systemu logowania wysyłanego do odbiorcy.
   8. Oferowane oprogramowanie musi umożliwiać łatwą korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację.
   9. Oferowane oprogramowanie musi posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora.
   10. Oferowane oprogramowanie musi umożliwiać łatwe i szybkie przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria.
   11. Oferowane oprogramowanie musi posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej.
   12. Oferowane oprogramowanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, takich jak np. logi aplikacji, logi sieciowe, pliki konfiguracyjne, informacje, dane wydajnościowe, zrzuty awaryjne itp., a także logów nieustrukturyzowanych.
   13. Oferowane oprogramowanie musi umożliwiać definiowanie struktury dla logów nieustrukturyzowanych.
   14. Oferowane oprogramowanie musi mieć możliwość raportowania utylizacji klastra wytworzonego na potrzeby przyjmowania dużych obciążeń EPS oraz przedstawiania tego zużycia w postaci grafów.
   15. Oferowane oprogramowanie musi dawać możliwość zabezpieczenia kanału wysyłania logów na zewnątrz oprogramowania za pomocą SSL.
   16. Oferowane oprogramowanie musi mieć możliwość granularnej aktualizacji pojedynczych agentów zainstalowanych na systemach operacyjnych.
   17. W zaoferowanym oprogramowaniu uprawnienia do interfejsu prezentacji i analizy logów muszą dopuszczać rozłączność z uprawnieniami do infrastruktury, z której zbierane są logi.
   18. Oferowane oprogramowanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami. Oprogramowanie musi pozwalać na tworzenie raportów, które można wysyłać za pomocą zdefiniowanych parametrów czasowych (ang. schedule) .
   19. Oferowane oprogramowanie musi zapewniać możliwość stworzenie klastra składającego się z minimum 15 węzłów, z którego każdy ma wydajność 15 000 EPS (ang. Events Per Second), co sumarycznie daje 250 000 EPS oraz 50 TB przestrzeni dyskowej.
   20. Oferowane oprogramowanie musi zapewniać wsparcie dla transformacji logów takich jak: filtrowanie logów (Log Filtering), przekazywanie logów do innych systemów (Forwarding) i maskowanie logów (Masking).
   21. Oferowane oprogramowanie musi posiadać możliwość logowania zdarzeń z platformy Kubernetes za pomocą agenta fluentd.
   22. Oferowane oprogramowanie musi mieć możliwość określania czasu retencji danych, tzn. Administrator w konsoli graficznej do zarządzania platformą do zbierania i korelacji logów musi mieć możliwość określenia czasu po jakim zebrane logi będą archiwizowane (eksportowane) na zewnętrznej macierzy dyskowej po protokole NFS. Dodatkowo wymaga się aby retencja mogła być ustawiana granularnie, tj. np. inny czas retencji dla logów z urządzeń klasy firewall a inny czas retencji dla logów z hyperwizorów.
   23. Oferowane oprogramowanie musi mieć możliwość instalacji swoich agentów na systemach operacyjnych Windows i Linux w celu zbierania z nich logów. Oferowane oprogramowanie musi posiadać możliwość granularnej aktualizacji poszczególnych agentów zainstalowanych na systemach operacyjnych.
   24. Oferowane oprogramowanie musi umożliwiać wygenerowanie na podstawie odbieranych danych eksportowanie zdefiniowanych raportów poprzez email na podstawie ustalonych zmiennych.
9. W zakresie platformy konteneryzacyjnej opartej na Kubernetes Zamawiający wymaga:
   1. Oferowane oprogramowanie musi być certyfikowane przez Cloud Native Computing Foundation (CNCF) w ramach programu certyfikacji zgodności z oprogramowaniem Kubernetes. Link to strony CNCF <https://www.cncf.io/certification/software-conformance/>.
   2. Licencje zaoferowanego oprogramowania muszą być równe liczbie zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.
   3. Platforma musi umożliwiać deklaratywne definiowanie limitów zasobów systemowych takich jak pamięć RAM i moc procesora, które będą dostępne dla projektu (grupy obiektów tj. wiele klastrów Kubernetes, maszyn wirtualnych), jak i dla poszczególnych kontenerów aplikacji.
   4. Platforma musi umożliwiać automatyczne tworzenie i zarządzanie minimum 100 klastrami Kubernetes dla klastra obliczeniowego. Licencja wraz ze wsparciem technicznym nie może ograniczać w żaden sposób tej ilości.
   5. Platforma musi umożliwiać uruchamianie wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych umożliwiając budowanie aplikacji pracujących w oparciu o maszyny wirtualne oraz mikro-serwisy.
   6. Platforma do automatycznego tworzenia i zarządzania klastrami Kubernetes musi posiadać narzędzia do zarządzania infrastrukturą (automatyczne tworzenie klastrów Kubernetes, modyfikowanie ilości węzłów i ich wielkości (moc CPU, pojemność RAM, pojemność dyskowa), usuwanie klastrów Kubernetes, aktualizowanie do nowszej wersji klastrów Kubernetes) poprzez Cluster API wraz ze wsparciem technicznym producenta całości oferowanej platformy.
   7. Platforma musi zapewniać środowisko wykonawcze kontenera, które umożliwia interakcję z wtyczkami sieciowymi (w standardzie CNI) i pamięcią masową (w standardzie CSI).
   8. Platforma musi posiadać możliwość wyboru co najmniej dwóch różnych rodzajów oprogramowania sieciowego w ramach automatycznego tworzenia klastra Kubernetes przez użytkownika platformy poprzez interfejs CNI. Dodatkowo musi być wspierana integracja z zewnętrznym (poza Kubernetes) rozwiązaniem klasy SDN (ang. Software Defined Network) dostarczonym do SDDC, tak aby była możliwość tworzenia polityk bezpieczeństwa z poziomu rozwiązania SDN.
   9. Platforma poprzez zintegrowaną wtyczkę CSI musi umożliwiać realizowanie trwałych zasobów bezpośrednio na kompatybilnej pamięci masowej SDS.
   10. Platforma do tworzenia i zarządzania klastrami Kubernetes musi umożliwiać pracę w środowiskach zamkniętych (ang. air-gapped enviroments).
   11. Platforma musi umożliwiać przesyłanie logów do zewnętrznych systemów logowania w tym dostarczonych.
   12. Platforma musi umożliwiać budowanie i uruchamianie aplikacji stanowych i bezstanowych na bazie orkiestratora Kubernetes. Orkiestrator Kubernetes musi posiadać wsparcie producenta oprogramowania dla jednego stosu SDDC.
   13. Platforma musi umożliwiać izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików.
   14. Platforma powinna zapewniać przekazywanie danych do systemu SIEM.
   15. Platforma musi mieć możliwość uruchomienia i zarządzania w chmurze prywatnej opartej o wirtualizator dostarczony.
10. W zakresie tworzenia i zarządzania sieciami wirtualnymi SDN Zamawiający wymaga:
    1. Oferowane oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne zbudowane na bazie rozwiązania wirtualizatora mocy obliczeniowej zaoferowanego w przedmiotowym postępowaniu.
    2. Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych.
    3. Oferowane oprogramowanie musi posiadać funkcję tworzenia rozproszonego, wirtualnego przełącznika instalowanego bezpośrednio w jądrze wirtualizatora serwerów (Hypervisor), umożliwiającego tworzenie logicznych segmentów sieci w warstwie L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta platformy wirtualizacyjnej serwerów.
    4. Oferowane oprogramowanie musi posiadać funkcję tworzenia rozproszonego, wirtualnego routera instalowanego bezpośrednio w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska serwerów wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów w warstwie sieci L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników (tj. poza środowisko wirtualizacyjne) skracając ścieżkę komunikacyjną i czas.
    5. Oferowane oprogramowanie musi posiadać możliwość kreowania segmentów sieci wirtualnej przy użyciu technologii GENEVE (Generic Network Virtualization Encapsulation) lub równoważnej.
    6. Oferowane oprogramowanie musi zapewnić funkcjonalność łączenia (ang. bridging) środowiska zwirtualizowanego opartego o technologię GENEVE oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów.
    7. Oferowane oprogramowanie musi zapewniać funkcjonalność wirtualnego routera wspierającego protokół BGP, BFD.
    8. Oferowane oprogramowanie musi zapewniać funkcjonalność translowania adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego do środowiska wirtualnego (DNAT).
    9. Oferowane oprogramowanie musi posiadać funkcjonalność serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska obiektów w środowisku zwirtualizowanym.
    10. Oferowane oprogramowanie musi posiadać funkcjonalność REST API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji.
    11. Aktualizacje oferowanego oprogramowania powinny odbywać się poprzez portal służący do ich planowania i uruchamiania, dostarczany przez tego samego producenta oprogramowania. Portal musi umożliwiać przegląd wszystkich elementów systemu pod kątem ich aktualnej oraz przygotowanej do aktualizacji wersji. Portal musi oferować wskaźniki postępu aktualizacji, umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia konsystencji działania systemu przed oraz po aktualizacji.
    12. Oprogramowanie musi zapewniać wsparcie dla wykorzystania plików danych JSON.
    13. Oferowane oprogramowanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do tej wirtualnej maszyny po zmianie jej adresu IP w sposób nieautoryzowany.
    14. Oferowane oprogramowanie musi posiadać możliwość terminowania tuneli IPSec site-to-site z uwierzytelnieniem za pomocą współdzielonego klucza (pre shared key) lub certyfikatu.
    15. Oferowane oprogramowanie musi posiadać funkcjonalność wsparcia mechanizmu VRF w obrębie wirtualizacji sieci.
    16. Oferowane oprogramowanie musi posiadać funkcjonalność mechanizmu VPC znanego z AWS lub GCP w obrębie wirtualizacji sieci możliwość kreowania sieci Publicznych i Prywatnych w obrębie projektu.
    17. Oferowane oprogramowanie musi posiadać funkcjonalność REST API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji.
    18. Oferowane oprogramowanie musi posiadać funkcjonalność zarządzania wieloma instancjami (min. 3) lokalnych instancji oprogramowania.
    19. Oferowane oprogramowanie musi posiadać moduł wsparcia procesu poszukiwania błędów (troubleshooting).
    20. Oferowane oprogramowanie musi być rozszerzalne o funkcjonalności bezpieczeństwa sieciowego minimum IDS, IPS, URL Filtering, Malware Detection, Dekrypcja SSL poprzez licencje.
11. W zakresie monitorowania i analizowania sieci oraz polityk firewall w sieciach wirtualnych i fizycznych Zamawiający wymaga:
    1. Oferowane oprogramowanie musi mieć możliwość analizowania przepływów sieciowych (NetFlow lub IPFIX) w warstwie sieciowej wirtualizacji opartej o rozwiązanie Compute.
    2. Oferowane oprogramowanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego. Poprzez raporty przepływów Zamawiający rozumie informację o ruchu sieciowym z konkretnej maszyny wirtualnej do innej konkretnej maszyny wirtualnej.
    3. Oferowane oprogramowanie musi mieć możliwość posiadania wbudowanego kolektora zebranego ruchu sieciowego możliwego do użycia w celu analizy ruchu.
    4. Oferowane oprogramowanie musi mieć możliwość generowania rekomendacji dla reguł serwerów klasy ściana ogniowa na bazie zebranych wcześniej informacji o przepływach.
    5. Oferowane oprogramowanie musi mieć możliwość wizualizacji (przedstawienia w postaci graficznej) ścieżki logicznej i przejść w relacji maszyna wirtualna do maszyny wirtualnej, wskazania komponentów sieciowych w topologii logicznej i fizycznej uwzględniając przełączniki, routery, firewall’e wspierane przez oprogramowanie oraz połączenia między nimi z uwzględnieniem komponentów wirtualnych (minimum host i maszyna wirtualna).
    6. Oferowane oprogramowanie musi mieć możliwość wizualizacji w formie graficznej przepływów pomiędzy minimum sieciami wirtualnymi, podsieciami, zdefiniowanymi aplikacjami oraz grupami bezpieczeństwa.
    7. Oferowane oprogramowanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły, które w ciągu analizy ruchu znajdują się w kolejce analizy je poprzedzają.
    8. Oferowane oprogramowanie musi mieć możliwość wizualizacji aplikacji działających w sieci klienta oraz wizualizacji zależności zarówno, pomiędzy maszynami wirtualnymi należącymi do tej aplikacji jak i ruchem zewnętrznym, wychodzącym i wchodzącym do maszyn wirtualnych odpowiedzialnych za tą aplikacje wraz z geolokalizacją zapytań.
    9. Oferowane oprogramowanie musi posiadać funkcjonalność API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji.
    10. Oferowane oprogramowanie musi funkcje backup konfiguracji i odtworzenia.
    11. Oferowane oprogramowanie musi mieć możliwość analizowania przepływów sieciowych w warstwie sieciowej dla urządzeń posiadanych przez Zamawiającego (Juniper MX / QFX).
    12. Oferowane oprogramowanie musi posiadać moduł analityczny pozwalający określenie progów dla wolumenu ruchu powiązanego z danymi maszynami wirtualnymi, wykrywający w sposób automatyczny przekroczenia tych progów.
    13. Oferowane oprogramowanie musi posiadać funkcjonalność informowania o źródłach generujących największą liczbę ruchu sieciowego.
    14. Oferowane oprogramowanie musi posiadać moduł wsparcia procesu poszukiwania błędów (troubleshooting).
    15. Oferowane oprogramowanie musi wspierać proces automatycznego odkrywania infrastruktury sieciowej w obrębie wspieranych przez oprogramowanie urządzeń.
    16. Oferowane oprogramowanie musi wspierać mapę urządzeń sieciowych.
    17. Oferowane oprogramowanie musi wspierać proces automatycznego odkrywania i mapowania ruchu sieciowego aplikacji na podstawie wykrytych przepływów generowanych przez aplikację.
    18. Oferowane oprogramowanie musi posiadać możliwość wizualizacji przepływów sieciowych do klastrów kontenerów działających w oparciu o rozwiązanie Kubernetes.
    19. Oferowane oprogramowanie musi posiadać funkcjonalność konfigurowania i zarządzania okresem retencji gromadzonych danych.
    20. Oferowane oprogramowanie musi posiadać możliwość analizy i przedstawiania wyników z tej analizy dla ruchu sieciowego na podstawie fabrycznie zaimplementowanych wytycznych co do zgodności ze standardem bezpieczeństwa PCI (Payment Card Industry).
12. W zakresie wirtualizacji przestrzeni dyskowych SDS Zamawiający wymaga:
    1. Oferowane oprogramowanie musi umożliwiać zbudowania współdzielonej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych.
    2. Komponent do wirtualizacji przestrzeni dyskowych należy dostarczyć z licencjami na sumę dostępnych zasobów dyskowych RAW w TiB (Tebibajt).
    3. Ilość TiB zaoferowanego oprogramowania do wirtualizacji przestrzeni dyskowych SDS musi być równy liczbie fizycznych zasobów dyskowych dostarczonych do wirtualizacji mocy obliczeniowej.
    4. Każdy serwer fizyczny, na którym zostanie zainstalowane zaoferowane oprogramowanie, musi dostarczać zarówno moc obliczeniową do klastra (CPU i RAM), jak również przestrzeń dyskową definiowaną programowo (eng. Software Defined Storage). Powyższa funkcjonalność musi dać możliwość utworzenia przestrzeni dyskowej złożonej z 64 hostów.
    5. Oprogramowanie powinno wspierać konfiguracje typu all-flash - w oparciu o dyski SSD (SAS/SATA/NVMe).
    6. Oprogramowanie powinno wspierać konfiguracje złożone wyłącznie z dysków NVMe (o parametrach 3 DWPD - “drive writes per day” - lub 1 DWPD).
    7. W przypadku potrzeby wykonania rozwiązania opartego na zaoferowanym oprogramowaniu, posiadającego wyłącznie dyski SSD, Oferowane oprogramowanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji zapisu.
    8. Oferowane oprogramowanie musi wspierać technologie NVMe i “cache’owanie” operacji zapisu z wykorzystaniem dysków NVMe.
    9. Oferowane oprogramowanie musi pozwalać na wsparcie dla rozmiaru cache na poziomie minimum 1.6TB per grupa dyskowa dla posiadanych dysków.
    10. Oferowane oprogramowanie musi wspierać technologie NVMe i posiadać wbudowaną możliwość „cache’owania”, bez dedykowanych w tym celu dysków, dzięki czemu wszystkie potrzeby w zakresie wydajności i pojemności będą realizowane przez te same urządzenia pamięci masowej (dyski).
    11. Zaoferowane rozwiązanie musi umożliwiać konfigurację serwerów fizycznych klasy all-NVMe.
    12. W przypadku zastosowania dysków NVMe zaoferowanie oprogramowanie musi wspierać ich wymianę w trybie hot-plug dla dodawania i wyjmowania dysków “na gorąco”. Taka funkcjonalność musi być dostępna dla minimum dwóch producentów serwerów obecnych na rynku.
    13. Oferowane oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji pamięci masowej w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów na rynku.
    14. Oferowane oprogramowanie musi zapewniać możliwość zmniejszania lub zwiększenia przestrzeni dyskowej (odjęcie lub dodanie pojedynczego dysku, odjęcie lub dodanie serwera fizycznego) w sposób niewymagający przestoju i przerwy w dostępie do działających na zmienianym środowisku maszyn wirtualnych.
    15. Oferowane oprogramowanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji lub konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania lub dodatkowych maszyn wirtualnych.
    16. Konfiguracja, zarządzanie i monitoring przestrzeni dyskowej, w zaoferowanym oprogramowaniu, muszą być zintegrowane z centralną konsolą zarządzającą platformą wirtualizacyjną.
    17. Oferowane oprogramowanie musi zapewniać możliwość obsługiwania dysków wirtualnych maszyn minimum dla rozmiaru 60TB.
    18. Funkcjonalności zaoferowanego oprogramowania nie może w żaden sposób ograniczać lub niwelować żadnej funkcjonalności platformy wirtualizacyjnej między innymi w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
    19. Oferowane oprogramowanie musi zapewniać funkcjonalność konfigurowalnych mechanizmów zabezpieczania danych na wypadek awarii sprzętowej w ramach lokalizacji lub szafy rack w taki sposób, aby poszczególne kopie dysków maszyny wirtualnej nie były umieszczane na hostach w ramach tej samej szafy rack lub w ramach tej samej lokalizacji.
    20. Oferowane oprogramowanie musi posiadać, na oficjalnej stronie producenta tego oprogramowania, listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 3 niezależnych producentów sprzętu serwerowego dostępnego na terenie Unii Europejskiej.
    21. Oferowane oprogramowanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery fizyczne producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery fizyczne, wytworzone na podstawie zaoferowanego oprogramowania, rozwiązanie nie może wprowadzać wymogu, aby w kolejnych dostarczanych serwerach fizycznych wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawcę/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery).
    22. Oferowane oprogramowanie musi zapewniać funkcjonalność możliwości rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej (w ramach istniejącej infrastruktury serwerów fizycznych) bez konieczności dodawania kolejnych serwerów fizycznych.
    23. Oferowane oprogramowanie musi zapewniać funkcjonalność możliwości rozbudowy i skalowania zarówno mocy obliczeniowej, jak i pojemności przestrzeni dyskowej (w ramach istniejącej infrastruktury serwerów fizycznych) bez konieczności dodawania kolejnych serwerów fizycznych.
    24. Oferowane oprogramowanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej poprzez dodanie pojedynczego dysku lub dodanie jednego lub więcej serwera fizycznego w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych.
    25. Oferowane oprogramowanie musi zapewniać możliwość ochrony danych przed utratą ich integralności za pomocą weryfikacji sum kontrolnych. Suma kontrolna musi być liczona w momencie wykonania przez maszynę wirtualną operacji IO write już na poziomie wirtualizatora.
    26. Oferowane oprogramowanie musi umożliwiać zarządzanie warstwą wirtualizacji mocy obliczeniowej i pamięci masowej bezpośrednio z interfejsu Webowego UI.
    27. Oferowane oprogramowanie musi umożliwiać tworzenie wysoko dostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. „oddziału zdalnego”, zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje. Architektura systemu musi mieć możliwość dołączania kolejnych lokalizacji „oddziałów zdalnych” w liczbie minimum 20.
    28. Oferowane oprogramowanie musi zapewniać natywną integrację (bez skryptów i/lub wtyczek programowych, ang. pluginów) z zaoferowanym w przedmiotowym postępowaniu komponentem do zarządzania klastrami wirtualizacyjnymi.
    29. Oferowane oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, stripes.
    30. Oferowane oprogramowanie musi posiadać możliwość udostępniania przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością bez konieczności wyłączania systemów na tej przestrzeni posadowionych („w locie”).
    31. Oferowane oprogramowanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji systemu.
    32. Oferowane oprogramowanie musi umożliwiać funkcjonalność automatycznego odzyskiwania pojemności dyskowej (przestrzeni dyskowej) zwolnionej na poziomie systemu operacyjnego tj. TRIM/UNMAP (ang. storage space reclamation).
    33. Oferowane oprogramowanie musi posiadać opcję wykorzystania natywnego dostawcy kluczy szyfrujących, jak również wykorzystania zewnętrznych dostawców.
    34. W zaoferowanym oprogramowaniu platforma zarządzania cyklem życia produktu musi wspierać co najmniej 3 różnych producentów serwerów.
    35. Oferowane oprogramowanie musi wspierać szyfrowanie na poziomie SHA256.
    36. Oferowane oprogramowanie musi mieć możliwość włączania na żądanie i wyłączania na żądanie dostępnej w ramach funkcjonalności zaoferowanego oprogramowania deduplikacji i kompresji.
    37. Oferowane oprogramowanie musi mieć możliwość włączania na żądanie i wyłączania na żądanie dostępnej w ramach funkcjonalności zaoferowanego oprogramowania kompresji.
    38. Oferowane oprogramowanie musi zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. erasure coding) dla RAID 5 i RAID 6, konfigurowane per pojedynczy dysk maszyny wirtualnej.
    39. Oferowane oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych z granulacją na poziomie dysków maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, stripes, replikację lub jej brak w ramach rozciągniętego klastra. Funkcjonalność klastra opisana została w poprzedzającym punkcie.
    40. Oferowane oprogramowanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek awarii jednego z dwóch centrów danych (klaster rozciągnięty) w taki sposób, aby poszczególne kopie maszyn wirtualnych były umieszczane zarówno na hostach w ramach tej samej lokalizacji (lokalna protekcja) oraz w ramach dwóch lokalizacji (protekcja na poziomie lokalizacji).
    41. Oferowane oprogramowanie musi umożliwiać szyfrowanie przestrzeni dyskowej przydzielonej do serwerów wirtualnych. Szyfrowanie nie może być realizowane poprzez dyski samoszyfrujące (ang. Self Encrypting Drives).
    42. Oferowane oprogramowanie musi posiadać możliwość uruchomienia usługi NFS w wersji 3 oraz 4.1. Ta usługa musi być zintegrowana z warstwą wirtualizacji oraz uruchamiania i zarządzana wyłącznie z poziomu centralnej konsoli zarządzającej klastrem wirtualizacyjnym bez potrzeby manualnej instalacji dodatkowych komponentów zewnętrznych.
    43. Oferowane oprogramowanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. erasure coding) dla RAID 5 i RAID 6, konfigurowane granularnie per zasób NFS/SMB share.
    44. Funkcjonalność usługi NFS w zaoferowanym oprogramowaniu musi współpracować z Kubernetes CSI driver (Container Storage Interface) w ten sposób, że zasoby NFS kreowane są i usuwane automatyczne z poziomu kontenerów.
    45. Oferowane oprogramowanie w architekturze 2 hostów w klastrze musi pozwalać na wykorzystanie usług plikowych.
    46. Oferowane oprogramowanie musi umożliwiać zamontowanie zdalnych magazynów danych utworzonych w infrastrukturze SDS do istniejącego wirtualizatora, bez potrzeby licencjonowania tegoż wirtualizatora.
    47. W zaoferowanym oprogramowaniu konfiguracja rozciągniętego klastra musi uwzględniać nie tylko różnorodne scenariusze awarii, ale również warunki odzyskiwania stanu zasobów sprzed awarii. Mechanizm umieszczania utrzyma stan maszyny wirtualnej w tej samej lokalizacji do momentu pełnej resynchronizacji danych, co zapewni, że wszystkie operacje odczytu nie będą przechodzić przez łącze między ośrodkami.
    48. Wsparcie dla funkcjonalności NFS/SMB może być realizowane w sieciach IPv6.
    49. Oprogramowanie musi zapewniać możliwość utworzenia i obsługi minimum 400 maszyn wirtualnych (ang. VM) na host.
    50. Oprogramowanie musi wspierać automatyczne zarządzanie domyślną polityką pamięci masowej, tym samym wspierać tworzenie i przypisywanie domyślnej polityki pamięci masowej zaprojektowanej automatycznie dla klastra - w oparciu o rozmiar i typ klastra, funkcja automatycznego zarządzania polityką musi wybierać idealny poziom tolerancji awarii i schemat umieszczania danych. Oprogramowanie musi umożliwiać monitorowanie i ostrzeganie użytkownika, jeśli domyślne zasady przechowywania są nieoptymalne.
    51. Oprogramowanie musi zapewniać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych (ang. erasure coding) dla RAID 5 przy użyciu trzech hostów.
    52. Oprogramowanie musi wspierać monitorowanie wydajności w czasie rzeczywistym oraz zbierać dane diagnostyczne co najmniej co 30 sekund.
    53. Oprogramowanie musi zapewniać możliwość wykonywania operacji deep rekey. Deep rekey odszyfrowuje dane, które zostały zaszyfrowane i zapisane przy użyciu starego klucza szyfrowania i ponownie szyfruje dane przy użyciu nowo wydanych kluczy szyfrowania przed zapisaniem ich w klastrze.
13. W zakresie siec SDN i bezpieczeństwa sieciowego Zamawiający wymaga:
    1. Oferowane oprogramowanie musi mieć wbudowany silnik IDS/IPS (Intrusion Detection System / Intrusion Prevention System).
       1. IPS/IDS w zaoferowanym oprogramowaniu musi działać na podstawie silników: sygnaturowego, dekodera protokołu oraz wykrywania anomalii.
       2. IPS/IDS w zaoferowanym oprogramowaniu musi działać w sposób granularny, tj. np. dawać możliwość przypisywania tylko polityki bazodanowej do tylko serwerów bazodanowych.
    2. Oferowane oprogramowanie musi posiadać silnik korelacji zdarzeń pochodzących między innymi z systemu IDS/IPS, detekcji malware, analizy ruchu sieciowego tj. modułu analizującego zdarzenia w sieci komputerowej.
    3. Oferowane oprogramowanie musi posiadać moduł Sandbox w celu analizy w środowisku kontrolowanym podejrzanych plików i oceny zagrożenia.
    4. Oferowane oprogramowanie musi posiadać funkcjonalność bezpieczeństwa sieciowego zarządzanego oraz instalowanego w ramach jednego interfejsu graficznego (pojedynczej konsoli).
    5. Oferowane oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego (vNIC) w hipervisorze wirtualizacyjnym dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym segmencie sieci Overlay i VLAN) bez wynoszenia ruchu do fizycznych przełączników lub firewalli na zewnątrz hypervisora.
    6. Oferowane oprogramowanie musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego bezpośrednio w jądrze wirtualizatora umożliwiającego tworzenie polityk bezpieczeństwa w warstwach ISO OSI 2, 3 i 4 oraz warstwie 7 z identyfikacją aplikacji.
    7. Filtracji ruchu sieciowego typu stanowy firewall.
    8. Oferowane oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i VLAN i na tym samym fizycznym serwerze (HCI)
    9. Oferowane oprogramowanie do tworzenia reguł polityk bezpieczeństwa, musi umożliwiać wykorzystanie, oprócz parametrów takich jak adres IP, porty i protokoły, dodatkowych obiektów, m. in.: nazwa maszyny wirtualnej, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny.
    10. Oferowane oprogramowanie musi zapewniać możliwość wdrożenia polityk bezpieczeństwa bez żadnych zmian w sieci fizycznej.
    11. Oferowane oprogramowanie musi mieć możliwość wizualizacji przepływów sieciowych pomiędzy maszynami wirtualnymi w środowisku, w którym zainstalowane jest oprogramowanie.
    12. Oferowane oprogramowanie musi mieć możliwość przeanalizowania ruchu powiązanego z wybraną grupą maszyn wirtualnych w zadanym okresie i na tej podstawie zarekomendowania reguł bezpieczeństwa polityki dla wybranej grupy maszyn wirtualnych.
    13. Oferowane oprogramowanie musi dawać możliwość przeprowadzenia symulacji jak będzie wyglądała komunikacja w ramach danej aplikacji po zastosowaniu rekomendowanych reguł bezpieczeństwa.
    14. Oferowane oprogramowanie musi umożliwiać implementację zarekomendowanych reguł bezpieczeństwa po uprzednim zatwierdzeniu ich przez administratora systemu.
    15. Oferowane oprogramowanie musi obejmować usługę pobierania informacji o podejrzanych adresach IP w sieci Internet, aby wdrożyć je jako element polityki bezpieczeństwa.
    16. Oferowane oprogramowanie musi posiadać funkcjonalność REST API umożliwiającą automatyzowanie wdrażania lub modyfikację konfiguracji.
14. W zakresie portalu samoobsługowego do automatycznego tworzenia maszyn wirtualnych w tym z bazami danymi MySQL i Postgres na dostarczonym module do wirtualizacji mocy obliczeniowej Zamawiający wymaga:
    1. Oferowane oprogramowanie musi posiadać funkcjonalność tworzenia gotowej maszyny wirtualnej z bazą danych MySQL lub/i Postgres z możliwością swobodnego dostosowania lub predefiniowanego rozmiaru zasobów obliczeniowych (maszyn wirtualnych) w zakresie wirtualnej pamięci oraz procesorów, w zależności od uprawnień użytkownika.
    2. Oferowane oprogramowanie musi posiadać funkcjonalność skalowania, czyli modyfikacji instancji maszyny wirtualnej z bazą danych MySQL lub/i Postgres w zależności od użycia (skalowanie w górę, skalowanie w dół, rozszerzenie dysku).
    3. Oferowane oprogramowanie musi posiadać funkcjonalność aktualizacji utworzonych maszyn wirtualnych z bazą danych MySQL lub/i Postgres poprzez planowanie instalacji poprawek i aktualizacji (w tym systemu operacyjnego), na żądanie lub według harmonogramu.
    4. Oferowane oprogramowanie musi posiadać funkcjonalność tworzenie kopii zapasowych, dzienników transakcji, odzyskiwanie punktu w czasie na żądanie lub według harmonogramu dla utworzonych baz danych MySQL lub/i Postgres.
    5. Oferowane oprogramowanie musi posiadać funkcjonalność tworzenie replikacja (zimna / gorąca lub repliki do odczytu) w zarządzanych strefach.
    6. Oferowane oprogramowanie musi posiadać funkcjonalność monitorowanie silnika bazy danych (MySQL i Postgres) oraz infrastruktury wirtualnej Compute.
    7. Oferowane oprogramowanie musi posiadać dla wyżej wymienionych funkcjonalności interfejs graficzny wytworzony w HTML5, tzn. portal samoobsługowy.
15. Wsparcie serwisowego Producenta dla Oprogramowanie do tworzenia i użytkowania chmury prywatnej SDDC.
    1. Zaoferowana usługa wsparcia serwisowego dla oferowanego oprogramowania musi być świadczona przez wyłącznie jeden podmiot lub organizację reprezentującą jeden podmiot na każdym etapie procesowania zgłoszenia. W łańcuchu obsługi zgłoszenia serwisowego, Zamawiający wyklucza możliwość przekazywania zgłoszeń serwisowych pomiędzy różnymi podmiotami. Zamawiający wyklucza również możliwość wykupienia usługi serwisowej przez Wykonawcę u partnera typu OEM (ang. Original Equipment Manufacturer) producenta przedmiotowego oprogramowania. Wsparcie serwisowe musi być składową zaoferowanych licencji w ramach czasu obowiązywania Umowy.
    2. Zaoferowana usługa wsparcia musi zapewniać poufność komunikacji na ewentualnych, poszczególnych etapach procedowania zgłoszenia. Nie dopuszcza się procesowania zgłoszeń serwisowych w systemach informatycznych nie zarządzanych przez producenta zaoferowanego oprogramowania.
    3. Zaoferowana usługa wsparcia serwisowego musi umożliwiać zgłaszanie problemów 7 dni w tygodniu, całodobowo, bez ograniczeń czasowych (7/24 – 24 godziny w ciągu doby przez 7 dni w tygodniu).
    4. Zaoferowana usługa serwisowa, w przypadku zgłoszenia o priorytecie 1 (najwyższym), musi być realizowana na zasadach „idź za słońcem” (ang. follow the sun) tj. inżynierów rozwiązujących zgłoszony problem w trybie 7/24 (24 godziny w ciągu doby przez 7 dni w tygodniu).
    5. Opis zaoferowanej usługi wsparcia serwisowego musi być dostępny na oficjalnej stronie internetowej producenta przedmiotowego oprogramowania.
    6. Usługa wsparcia serwisowego musi spełniać poniższe cechy:
       1. wykonywanie przez Zamawiającego nieograniczonej ilości zgłoszeń serwisowych,
       2. możliwość zapotrzebowania przez Zamawiającego wsparcia zdalnego,
       3. dostęp dla Zamawiającego do materiałów producenta oprogramowania, do którego oferowane jest przedmiotowe wsparcie, takich jak: techniczna dokumentacja, internetowa baza wiedzy,
       4. dostęp dla Zamawiającego do poprawek i uaktualnień oprogramowania objętego usługą wsparcia serwisowego,
       5. dostęp do portalu internetowego umożliwiającego zarządzanie posiadanymi przez Zamawiającego licencjami, utworzenie zgłoszenia serwisowego oraz pobierania kluczy licencyjnych,
       6. portal serwisowy udostępniony dla Zamawiającego w Internecie musi udostępniać założenie i wysłanie zgłoszenia (bez limitu ilości zgłoszeń),
       7. Wsparcie serwisowe musi posiadać priorytetyzację od poziomu 1 - najwyższego (Severity 1) do poziomu 4 - najniższego (Severity 4).

# Usługi w ramach Prac Zleconych

Poniżej szczegółowe wymagania w zakresie wymagań Usług realizowanych w ramach Umowy.

### Zakres Prac Zleconych:

1. W każdym z obszarów objętych Umową Wykonawca będzie posiadał certyfikowanych inżynierów w obszarze technologii stosowanych i oferowanych:
   1. Urządzeń HCI będzie posiadał minimum dwóch doświadczonych inżynierów w zakresie urządzeń firmy Dell Technologies, realizujących proces naprawy, instalacji, modyfikacji komplementów serwerów.
   2. Certyfikowanych (nie dalej jak w 2022 roku) minimum 3 inżynierów z zakresie produktów VMware lub równoważnych, posiadających łącznie doświadczenie w zakresie:
      1. z obszaru Compute i Storage: VMware Certified Professional - Data Center Virtualization lub równoważny certyfikat dla zaoferowanego oprogramowania;
      2. z obszaru Network: VMware Certified Professional - Network Virtualization lub równoważny certyfikat dla zaoferowanego oprogramowania;
      3. z obszaru Automation i Operation: inżynierów z co najmniej 5 letnim doświadczeniem w zakresie oferowanego oprogramowania.
      4. z obszaru Cloud Native: VMware Certified Professional - Application Modernization, Certified Kubernetes Administrator lub równoważny certyfikat dla zaoferowanego oprogramowania;
      5. z obszaru Projektowania DC / SDDC: VMware Certified Professional - Data Center Virtualization lub VMware Cloud Foundation Architect lub równoważny certyfikat dla zaoferowanego oprogramowania;
      6. Wiodący lider Expert w obszarze SDDC z co najmniej 10 letnim doświadczeniem lub posiadający certyfikat na poziomie Experta dla oferowanego oprogramowania
2. Prace zlecone będą obejmowały czynności dotyczące Oprogramowania SDDC w ramach Chmury Prywatnej m.in. konfiguracji, usług, integracji, dostosowania, adaptacji i strojenia do potrzeb Zamawiającego.
3. Przedmiotem czynności wykonywanych w ramach Prac Zleconych, mogą być w szczególności:
4. rekonfiguracja, rozwój, zmiany, konfiguracje i modyfikacje Oprogramowania i urządzeń Systemu w ramach lokalizacji OPD i ROPD (Załączniki H1),
5. przenosiny elementów Oprogramowania i urządzeń pomiędzy obszarami lokalizacjami Systemu,
6. ocena efektywności działania analizy z zakresie zgłoszonych zagadnień,
7. asysta techniczna na etapie przygotowań i testów poziomu niezawodności mechanizmów przełączania zasobów pomiędzy OPD i w ramach lokalizacji OPD,
8. wsparcie techniczne w testach niezawodności mechanizmów tworzenia kopii danych konfiguracji i ich odtwarzania dla oprogramowania SDDC i urządzeń,
9. przedstawienie wniosków i rekomendacji w zakresie rekomendowanych i uzasadnionych zmian dotyczących SDDC/urządzeń lub z nim związanych oraz wskazaniem kierunku proponowanych zmian/rozwoju wraz z uzasadnieniem,
10. integracje rozwiązań z systemami Zamawiającego,
11. uruchamianie przez Wykonawcę nowych funkcjonalności, zgodnie z dyspozycją Zamawiającego, a w przypadku konieczności zapewnienia dodatkowych licencji/subskrypcji do uruchomienia funkcjonalności realizacja prac odbędzie się po ich zapewnieniu przez Zamawiającego,
12. modyfikacje wynikające z rozbudowy,
13. szkoleń instruktażowych w ramach wykonanych zadań i technologii dostarczonych,
14. aktualizacji i instalacji poprawek systemowych w ramach Oprogramowania i urządzeń,
15. inne prace związane z Chmurą Prywatną zlecone Wykonawcy,
16. wykonywanie aktualizacji Dokumentacji i procedur operacyjnych,
17. sporządzenie cyklicznych raportów i analiz,
18. strojenie narzędzi do aktualnych potrzeb i zadań zgodnie ze zleceniami,
19. wykonywanie testów, PoC, PoV,
20. implementacje rozwiązań rozpoczynając od procesu testowania w środowisku testowym OPT,
21. w przypadku relokacji urządzeń Wykonawca dostarczy odpowiednie brakujące kable przyłączeniowe w ramach potrzeb lokalnych,
22. aktywną współpracę z innymi podmiotami zaangażowanymi, procesy zmian dla Chmury Prywatnej,
23. inne zadania wskazane w niniejszym dokumencie.

### Zlecanie Prac Zleconych:

1. Prace będą zlecane Wykonawcy drogą mailową lub w systemie zgłoszeń Wykonawcy przez osoby wskazane przez Zamawiającego, wraz ze wskazaniem ich zakresu i proponowanego przez Zamawiającego rezultatu oraz oczekiwanego terminu ich wykonania.
2. Wykonawca przekazuje Zamawiającemu potwierdzenie przyjęcia zgłoszenia, zgodnie z Czasem Reakcji.
3. Wykonawca przekazuje Zamawiającemu plan prac zawierający wykonanie pełnej i szczegółowej analizy wpływu implementowanych zmian w Chmurze Prywatnej na jego dotychczasowe funkcjonowanie i przedstawienie Zamawiającemu do akceptacji wraz z niezbędną liczbą godzin potrzebnych do realizacji prac, zgodnie z Czasem Odpowiedzi Wykonawcy.
4. Ostateczny zakres prac oraz terminy realizacji w ramach usługi Prac Zleconych będą uzgadniane przez Zamawiającego i Wykonawcę, co zostanie potwierdzone drogą mailową lub w systemie zgłoszeń Wykonawcy.
5. Strony dopuszczają zmianę kanału komunikacji na ustalony wspólnie w trybie roboczym.
6. Wykonawca rejestruje usługi Prac Zleconych w celach raportowych oraz odbiorczych.
7. Prace zadania podlegają usługom serwisowym Gwarancyjnym i Pogwarancyjnym w zależności od obszaru zadania.

### Poziomy świadczenia usługi Prac Zleconych

1. Wykonawca gwarantuje następujące poziomy świadczenia usługi.

|  | **Prace Zlecone** |
| --- | --- |
| **Czas Reakcji** | 1 dzień roboczy |
| **Czas Odpowiedzi Wykonawcy** | 5 dni roboczych |
| **Czas Zakończenia Realizacji Zadania** | 3 tygodni, jeżeli Zamawiający nie ustali innego terminu w ramach konsultacji z Wykonawcą |

Czas Reakcji:

1. Czas reakcji liczony jest od momentu zgłoszenia skierowanego do Wykonawcy przez Zamawiającego, do momentu poinformowania Zamawiającego przez Wykonawcę o przyjęciu zgłoszenia i podjęciu przez Wykonawcę czynności mających na celu jej realizacji.
2. Wykonawca informuje Zamawiającego o przyjęciu zgłoszenia poprzez umieszczenie odpowiedniej informacji w systemie zgłoszeń.

Czas Odpowiedzi Wykonawcy:

1. Czas realizacji zgłoszenia mierzony jest oddzielnie dla każdego zgłoszenia,
2. Czas realizacji zgłoszenia liczony jest od momentu zgłoszenia do momentu udzielenia odpowiedzi Zamawiającemu przez Wykonawcę,
3. Czas potwierdzenia przez Zamawiającego do Wykonawcy sposobu realizacji zgłoszenia Prac Zleconych, nie jest wliczany do czasu odpowiedzi Wykonawcy – na ten czas Wykonawca zawiesza zgłoszenie,
4. W przypadku skierowania przez Zamawiającego do Wykonawcy uwag do przedstawionego sposobu realizacji, Wykonawca odwiesza zgłoszenie i Czas Odpowiedzi Wykonawcy jest liczony od momentu udzielenia przez Zamawiającego uwag.

### Realizacja Prac Zleconych

1. Zamawiający umożliwi Wykonawcy realizację zleconych prac poprzez udostępnienie uzgodnionych zasobów.
2. Wykonawca zapewni osobę (opiekuna) do zgłoszonej pracy zleconej.
3. Zamawiający i Wykonawca współpracują w ramach realizacji Prac Zleconych.
4. Zmiany w Oprogramowaniu powinny być zrealizowane w pierwszej kolejności środowisku testowym (w szczególnych przypadkach może być dopuszczony na środowisku produkcyjnym po uprzednim zatwierdzeniu przez Zamawiającego).
5. Prace realizowane są z zachowaniem 50% niezmienności w infrastrukturze Chmury Prywatnej, jeśli jest to możliwe.
6. Prace realizowane są w godzinach ustalonych m.in. serwisowych i nocnych, jeżeli przedmiot prac obejmuje ryzyko niedostępności i wymaga pracy w oknie serwisowym.
7. Po wykonanych zmianach Wykonawca wspólnie z Zamawiającym przeprowadzi testy.
8. Wszelkie zrealizowane prace przez Wykonawcę w ramach Prac Zleconych zadania, objęte będą Gwarancją, której bieg rozpoczyna się od daty odbioru Prac Zleconych bez uwag.

### Testy Odbiorcze dla Prac Zleconych

1. Po wykonaniu czynności wchodzących w zakres Prac Zleconych, Strony ustalają zakres testów odbioru dla zrealizowanego zadania.
2. Czynności przygotowawcze do przeprowadzenia testów realizowane są przez Wykonawcę na postawie wskazanego przez Zamawiającego zakresu testów.
3. Testy odbywają w ciągu tygodnia po zakończeniu prac lub wyznaczonym terminie przez Zamawiającego.
4. Testy odbiorcze mają za zadanie potwierdzić zgodność zrealizowanych zadań ze zleceniem, sprawdzenie założeń i efektu, weryfikacja błędów.
5. Z testów sporządzana jest notatka lub protokół testów w zależności od zakresu czynności objętych pracami i poziomu wymaganych weryfikacji.
6. Testy odbiorcze może przeprowadzić Wykonawca i omówić jest w trakcie Odbioru Prac przy akceptacji Zamawiającego.
7. Odbiór szczegółowy realizowany jest głównie dla zadań złożonych o znacznym poziomie złożoności.

### Odbiór Prac Zleconych

1. Po wykonaniu czynności wchodzących w zakres Prac Zleconych, Strony sporządzą protokół odbioru czynności wraz ze wskazaniem liczby godzin roboczych przeznaczonych na wykonanie zleconych prac.
2. Czas realizacji poszczególnych prac (realizowanych na podstawie odrębnych zgłoszeń Zamawiającego) będzie zaokrąglany w górę z dokładnością do jednej roboczogodziny.
3. W ramach odbioru prac wykonywane są testy zlecone przez Zamawiającego, wyniki ich dołączane są do podsumowania zadań.
4. Wykonawca po realizacji prac dokona aktualizacji Dokumentacji Technicznej, o ile w wyniku zrealizowanych prac Dokumentacja powinna zostać zaktualizowana.

# Usługi Serwisowe

Wykonawca w okresie umowy realizuje usługi Serwisowe Gwarancyjne i Usługi Serwisowe Pogwarancyjne) na rzecz Zamawiającego zgodnie z dwoma poziomami jakości ich świadczenia, przedstawionymi poniżej:

1. w przypadku urządzeń i oprogramowania nie objętego usługami serwisowymi producenta realizowane są usługi w ramach Serwisu Pogwarancyjnego wsparcia infrastruktury zgodnie z pkt 9 – niższy poziom świadczenia usług.
2. dla urządzeń i oprogramowania objętego usługami serwisowymi producenta realizowane są usługi w ramach Serwisu Gwarancyjnego zgodnie z pkt 10 – wysoki poziom świadczenia usług.

# Serwis Pogwarancyjny

Usługa pogwarancyjna realizowana przez Wykonawcę polega na świadczeniu usług serwisowych dla oprogramowania VMware w ramach lokalizacji ROPD Systemu i urządzeń Systemu wymienionych w Załączniku H1.

Okres świadczenia Serwisu Pogwarancyjnego rozpoczyna się wraz z podpisaniem Umowy i trwa do 31.12.2027 roku.

1. W ramach Serwisu Pogwarancyjnego, Wykonawca zobowiązany jest do:
   1. diagnostyki i proponowania rozwiązań dla Problemów zgłaszanych przez Zamawiającego w ramach oprogramowania i urządzeń,
   2. instalacji i integracji oprogramowania w tym Oprogramowania SDDC wyniku awarii urządzenia celem usunięcia awarii,
   3. wsparcia w instalacji oprogramowania, tj.:
      1. oferowanego przez producenta w ramach licencji wieczystych po ustaniu serwisu producenta,
   4. udzielania Konsultacji w obrębie przedmiotu realizowanej usługi,
   5. wykonania obowiązków opisanych w SOPZ w terminie podanym jako nieprzekraczalny obejmujący zadania zlecone i modyfikacje dla Chmury Prywatnej OPD,
   6. utrzymywania Dostępności uruchomionych urządzeń Zamawiającego pracujących w ramach lokalizacji OPD, ROPD i pozostałych, poprzez realizacje czynności zmierzających do naprawy urządzeń wykorzystywanych produkcyjnie przy wykorzystaniu części zamiennych ze stoku Zamawiającego (co najmniej 10% urządzeń (serwerów) zostanie przeznaczonych jako stok urządzeń zamiennych),
   7. stok urządzeń będzie zrealizowany głównie w lokalizacjach OPD1, OPD2 i pojedynczych serwerów dla lokalizacji ROPD,
   8. naprawa urządzeń będzie realizowana zgodnie z dyspozycjami Zamawiającego.
2. Wykonawca zobowiązuje się, iż objęte w ramach Umowy urządzenia będą serwisowane zgodnie z wymaganiami przedstawionymi w zakresie:
   1. Przyjęcie zgłoszenia zgodnie z kategorią Problemu.
   2. Przeprowadzenie analizy Problemu zdalnej lub lokalnej diagnostyki.
   3. Zaproponowanie sposobu obejścia i naprawy Problemu.
   4. Docelowa naprawa zgłoszonego Problemu zgodnie z określonymi czasami i decyzją Zamawiającego.
3. Wszelkie koszty rozwiązywania Problemów, w tym koszt testów, dojazdu, instalacji i uruchomienia urządzenia ponosi Wykonawca.
4. Wykonawca i Zamawiający współpracują przy rozwiązywaniu Problemów.
5. Wykonawca współpracuje przy rozwiązywaniu Problemów z innymi podmiotami odpowiedzialnymi za pozostały obszar Systemu m.in. urządzenia, kopie zapasowe i odzyskiwanie.
6. Pogwarancyjna usługa udzielona przez Wykonawcę musi obejmować m.in:
   1. dostęp do portalu internetowego umożliwiającego zarządzanie zgłoszeniami i stanem ilościowym urządzeń Zamawiającego, utworzenie zgłoszenia serwisowego, procesowanie zgłoszenia i archiwizację złożonych awarii z procesem naprawy w okresie realizacji usługi.
7. Wykonawca zapewni zdalne wsparcie tożsame z usługą Serwisu Gwarancyjnego.

### Ogólne warunki Serwisu Pogwarancyjnego

**9.1.1 Diagnostyka i Rozwiązywanie Problemów**

W zakresie wsparcia Serwisu Pogwarancyjnego Wykonawca zapewnia Zamawiającemu usługę diagnostyki i Rozwiązywania Problemów w ramach urządzeń Chmury Prywatnej i lokalizacji ROPD.

**9.1.1.1    Klasyfikacja Problemów**

Klasyfikację Problemów określa Zamawiający z priorytetem realizacji. W przypadku, gdy Strony zgodzą się, do zmiany w kolejności procesowania zgłoszeń celem optymalizacji i przywrócenia dostępności Urządzeń i funkcjonalności oprogramowania, Zamawiający może zaakceptować propozycje Wykonawcy.

***Awaria urządzenia*** - wystąpienie problemu o znaczeniu krytycznym, powodując niedostępność usług i / lub operacji. Możliwe ograniczenia w funkcjonowaniu lokalizacji. Spełniona zostaje jedna z wymienionych niżej przesłanek:

1. utrudnia funkcjonowanie lokalizacji OPD, ogranicza wydajność lub bezpieczeństwo danych,
2. nie jest możliwe korzystanie z urządzenia – serwera,
3. występuje brak komunikacji z urządzeniem – serwerem;
4. urządzenie powoduje problem ze stabilnością (OPD, ROPD), wymagane jest jego wyłączenie;

nie jest możliwe stwierdzenie stanu urządzenia.

***Awaria komponentu urządzenia*** - wystąpienie problemu, w którym występuje zakłócenie usługi i / lub operacji. Spełniona zostaje jedna z wymienionych niżej przesłanek:

1. brak możliwości zarządzania urządzeniem w ROPD,
2. brak stabilności w zarządzaniu oprogramowaniem / urządzeniem,
3. brak możliwości realizacji usług przez urządzenie w ważnym miejscu Chmury Prywatnej,
4. występują utrudnienia z elementami serwera powodujące niestabilność dla lokalizacji;

***Awaria funkcjonalności*** - wystąpienie problemu z oprogramowaniem o znaczeniu poważnym, powodując utrudnienia usług i / lub operacji. Możliwe ograniczenia w funkcjonowaniu lokalizacji. Spełniona zostaje jedna z wymienionych niżej przesłanek:

1. dotyczy lokalizacji ROPD,
2. występuje problem w obszarze Compute / SDS / Network utrudniający funkcjonowanie lokalizacji,
3. występuje niestabilność lokalizacji utrudniająca funkcjonowanie usług;

***Usterka*** – pozostałe Problemy z urządzeniem m.in.:

1. niedostępność, która nie wpływa negatywnie na funkcjonowanie lokalizacji OPD, ROPD,
2. problem ze spadkiem wydajności wydłużający czas odpowiedzi lub poziom bezpieczeństwa np. danych,
3. uszkodzenia wkładki, dysku, kabla transmisyjnego/przyłączeniowego do serwera
4. utrudnienia w monitorowaniu, raportowaniu stanu,
5. problem z integracjami,
6. inne nie wpływające na funkcjonowanie serwera.

**9.1.1.2    Poziomy świadczenia usługi**

W zależności od klasyfikacji Problemu, Wykonawca gwarantuje następujący czas realizacji Zgłoszeń Zamawiającego:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Klasa problemu | **Maksymalny czas reakcji na zgłoszenie** | **Maksymalny czas przywrócenia**  **normalnego działania/Rozwiązania Problemu (\*)** | **Maksymalny czas dostarczenia rozwiązania docelowego (\*\*)** | **Tryb serwisowania** |
| Awaria urządzenia | 8 godzina | 24 godziny | 3 dni robocze | 24x7 |
| Awaria komponentu urządzenia | 8 godziny | 48 godzin | 5 dni roboczych | 24x7 |
| Awaria funkcjonalności | 8 godziny | 72 godzin | 14 dni \*\*\* roboczych  testy funkcjonalne | 8x5 |
| Usterka | 24 godziny | 5 dni | 10 dni w ramach dostępność części | 8x5 |

\* również zastosowanie Obejścia

\*\* w przypadku zastosowania Obejścia

\*\*\* w przypadku braku błędu po stronie producenta

**Pozostałe wymagania w zakresie:**

* procesowania zgłoszeń
* wymiany informacji między Stronami.
* Zgłoszenia Problemów itp.
* Konsultacje
* Raportowanie usług pogwarancyjnych

Będą realizowane zgodnie w opisem w punktu Serwis Gwarancyjny ppkt 10.2.1.3 i poniżej.

# Serwis Gwarancyjny

### Ogólne warunki Serwisu Gwarancyjnego

Serwis Gwarancyjny świadczony przez Wykonawcę na rzecz Zamawiającego polega na świadczeniu usług serwisowych dla Oprogramowania w ramach Chmury Prywatnej SDDC dla OPD z poziomami obsługi opisanymi w niniejszym dokumencie. Okres świadczenia Serwisu Gwarancyjnego rozpoczyna się wraz z podpisaniem Umowy i Protokołu Odbioru Opcji i trwa do 31.12.2027 r. lub zgodnie z zamówionym prawem Opcji.

1. W ramach Serwisu Gwarancyjnego, Wykonawca zobowiązany jest do:
   1. diagnostyki i Rozwiązywania Problemów zgłaszanych przez Zamawiającego w ramach Oprogramowania SDDC Chmury Prywatnej i jej składników, urządzeń,
   2. dostarczania i wsparcia w instalacji Oprogramowania, tj.:
   3. poprawek (Aktualizacji) Oprogramowania,
   4. najnowszych komercyjnie dostępnych wersji Oprogramowania wraz z obowiązkiem udzielenia niezbędnych licencji/subskrypcji, na zasadach określonych w Umowie, bez dodatkowych kosztów dla Zamawiającego,
   5. udzielania Konsultacji,
   6. wykonania obowiązków opisanych w SOPZ w terminie podanym jako nieprzekraczalny obejmujący proces implementacji Oprogramowania i wykonania integracji,
   7. utrzymywania Dostępności Oprogramowania Chmury Prywatnej,
2. Wykonawca gwarantuje, iż objęte w ramach Umowy wkładki optyczne QSFP i SFP+ i baterie podtrzymujące konfiguracje znajdujące się w urządzeniach zgodnie z załącznikiem H1 będą objęte usługą Serwisu Gwarancyjnego.
3. Wykonawca gwarantuje, iż objęte w ramach Umowy Oprogramowanie będzie objęte usługą Serwisu Gwarancyjnego.
4. W okresie Gwarancji Wykonawca będzie udostępniał Zamawiającemu dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej Oprogramowania.
5. Serwis Gwarancyjny na Oprogramowanie będzie świadczona w miejscu używania Oprogramowania.
6. Wszelkie koszty rozwiązywania Problemów, w tym koszt testów, instalacji i uruchomienia Oprogramowania ponosi Wykonawca.
7. Wykonawca i Zamawiający współpracują przy rozwiązywaniu Problemów.
8. Wykonawca współpracuje przy rozwiązywaniu Problemów z innymi podmiotami odpowiedzialnymi za pozostały obszar Systemu m.in. urządzenia, kopie zapasowe i odzyskiwanie.
9. W przypadku, gdy Wykonawca podczas realizacji usługi Serwisu Gwarancyjnego dostarczy nową wersję Oprogramowania, Wykonawca przeprowadzi proces testowania i weryfikacji celem sprawdzenia zgodności.
10. Zamawiający zobowiązany jest do przestrzegania reguł użytkowania i eksploatacji Oprogramowania, użytkowania go zgodnie z procedurami opisanymi w Dokumentacji Technicznej.
11. Zamawiający może dokonać rozbudowy Chmury Prywatnej bez utraty uprawnień wynikających z Serwisu Gwarancyjnego na Oprogramowanie dostarczone w ramach realizacji niniejszej Umowy.
12. Serwis Gwarancyjny udzielona przez Wykonawcę musi obejmować m.in:
    1. dostęp do portalu internetowego umożliwiającego zarządzanie posiadanymi przez Zamawiającego urządzeniami, utworzenie zgłoszenia serwisowego, procesowanie zgłoszenia i archiwizację złożonych awarii z procesem naprawy w okresie gwarancji.
13. Wykonawca zapewni zdalne wsparcie (poprzez platformę do współpracy, telefon lub e-mail) w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem Oprogramowania.
14. W przypadku licencji/subskrypcji czasowych datą aktywacji licencji/subskrypcji będzie data wskazana w SOPZ.

### Opis usług Serwisu Gwarancyjnego

**10.2.1 Diagnostyka i Rozwiązywanie Problemów**

W zakresie Serwisu Gwarancyjnego Wykonawca zapewnia Zamawiającemu usługę diagnostyki i Rozwiązywania Problemów w ramach Chmury Prywatnej.

**10.2.1.1    Klasyfikacja Problemów**

Klasyfikację Problemów określa Zamawiający. W przypadku, gdy Strony zgodzą się, że Chmura Prywatna pomimo zgłoszenia funkcjonuje prawidłowo, zgłoszenie to nie jest uznawane za awarię oraz nie jest wliczane do obliczeń w zakresie utrzymania dostępności Chmury Prywatnej.

***Awaria Krytyczna*** - wystąpienie Problemu o znaczeniu krytycznym dla Zamawiającego, powodująca poważne i szkodliwe zakłócenie usług i / lub operacji. Możliwe są duże straty finansowe, problemy z bezpieczeństwem, naruszenia zgodności, straty i szkody dla reputacji. Spełniona zostaje jedna z wymienionych niżej przesłanek:

* nie jest możliwe korzystanie przez Zamawiającego z Oprogramowania / Urządzeń w OPD w ramach posiadanej Chmury Prywatnej lub korzystanie z niego jest znacząco utrudnione (degradacja funkcjonalności);
* nie działają funkcjonalności Oprogramowania / Urządzeń i występuje ich znacząca degradacja w obu lokalizacjach OPD1 i 2;
* wydajność lub stabilność Oprogramowania / Urządzeń uległa obniżeniu, w stosunku do wartości początkowej;
* Oprogramowanie powoduje problem ze niestabilnością Chmury Prywatnej w OPD m.in. np. SDN/Sieci, dostępu do danych, wirtualizacji zasobów Compute Storage lub innych;
* Urządzenie powoduje problem ze stabilnością systemu backupu;

nie jest możliwe stwierdzenie stanu Chmury Prywatnej lub jego elementów.

***Awaria Poważna*** - wystąpienie Problemu, w którym występuje zakłócenie usługi i / lub operacji. Konsekwencje obejmują pewne straty finansowe, naruszenia zgodności, szkody dla reputacji i możliwe obawy dotyczące bezpieczeństwa. Spełniona zostaje jedna z wymienionych niżej przesłanek:

1. brak możliwości zarządzania Oprogramowaniem / Urządzeniem,
2. brak możliwości realizacji usług przez Chmurę Prywatną.
3. występują utrudnienia z elementami Oprogramowania / Urządzeniem powodujące niestabilność dla lokalizacji;

***Awaria Istotna***- wystąpienie Problemu w wyniku, którego powstają utrudnienia w dostępie do Oprogramowania / Urządzenia. Obejmuje przerwy w obsłudze użytkownika lub funkcjonalności, głównie o ograniczonym zakresie, czasie trwania lub skutku. Wpływ finansowy jest minimalny lub żaden. Spełniona zostaje jedna z wymienionych niżej przesłanek:

1. uszkodzenie Oprogramowania / Urządzenia lub jego elementów powodujące ograniczenie możliwości działania jego funkcjonalności, ale nieuniemożliwiające korzystania z Chmury Prywatnej,
2. Oprogramowanie, w którym część Chmury Prywatnej nie funkcjonuje zgodnie z dokumentacją aktualnie eksploatowanej wersji Oprogramowania, co utrudnia pracę co najmniej jednej z jego funkcjonalności,
3. spadek wydajności wydłużający czas odpowiedzi lub poziom bezpieczeństwa np. danych, niezawodności.

***Usterka*** – pozostałe Problemy m.in.:

1. problem z monitorowaniem, raportowaniem,
2. problem z integracjami,
3. Inne.

**10.2.1.2    Poziomy świadczenia usługi**

W zależności od klasyfikacji Problemu, Wykonawca gwarantuje następujący czas realizacji Zgłoszeń Zamawiającego:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Klasa problemu | Maksymalny czas reakcji na zgłoszenie | Maksymalny czas przywrócenia  normalnego działania/Rozwiązania Problemu (\*) | Maksymalny czas dostarczenia rozwiązania docelowego (\*\*) | Tryb serwisowania |
| Awaria Krytyczna | 2 godzina | 8 godziny | 2 dni robocze | 24x7 |
| Awaria Poważna | 4 godziny | 16 godzin | 5 dni roboczych | 24x7 |
| Awaria Istotna | 8 godzin | 24 godzin | 10 dni roboczych | 8x5 |
| Usterka | 24 godziny | 48 godzin | Następne planowe uaktualnienie  oprogramowania  ("Release" lub "update") | 8x5 |

\* również zastosowanie Obejścia

\*\* w przypadku zastosowania Obejścia

**10.2.1.3     Wymiana informacji między Stronami.**

1. Strony dopuszczają następujące kanały komunikacyjne:

* system zgłoszeń problemowych Wykonawcy,
* poczta elektroniczna,
* strona WWW,
* telefon
* komunikator typu **Teams**/Zoom/Webex.

1. Zgłoszenia kierowane przez Zamawiającego za pośrednictwem telefonu, będą również potwierdzane niezwłocznie, poprzez wysłanie e-mail do Wykonawcy z podaniem czasu zgłoszenia za pośrednictwem telefonu. W takiej sytuacji za czas Zgłoszenia Problemu, uważa się moment zgłoszenia za pośrednictwem telefonu.
2. Wykonawca zobowiązany jest przyjmować i rejestrować Zgłoszenia Problemów składane przez Zamawiającego w trybie 24/7/365.
3. Wykonawca będzie aktualizował wszelkie dane o Problemie - takie jak postępy prac, statusy, priorytet, typ - w systemie zgłoszeń problemowych, a cała historia korespondencji oraz statusów będzie dostępna dla Zamawiającego.
4. Wszelka korespondencja między stronami będzie odbywała się w języku polskim.
5. Szczegóły przekazania dostępów do systemu zgłoszeń problemowych Wykonawcy, zostaną przekazane Zamawiającemu w trybie roboczym.
6. Strony, w trakcie trwania Usług Gwarancji, mogą umówić się na integracje między systemami zgłoszeń problemowych Wykonawcy i Zamawiającego. Szczegóły zostaną uzgodnione w trybie roboczym.
7. Zamawiający dostarczy bezpieczny zdalny i nadzorowany dostęp do Oprogramowania w okresie obowiązywania umowy ustalony w trybie roboczym.

**10.2.1.4     Zgłoszenia Problemów**

1. Zamawiający jest odpowiedzialny za przekazanie w Zgłoszeniu Problemu kompletu informacji, w szczególności:

* osobę lub osoby kontaktowe reprezentujące Zamawiającego,
* identyfikację i lokalizację Urządzenia,
* opis Problemu,
* klasyfikację Problemu,

1. Za czas Zgłoszenia Problemu uznaje się moment skutecznego poinformowania Wykonawcy przez Zamawiającego o zaistniałym Problemie.
2. Za klasyfikację Problemu odpowiedzialny jest Zamawiający.
3. Wykonawca w trybie roboczym będzie przedstawiał swoje uwagi, gdy Problemy będą zgłaszane w sposób nieprawidłowy po Rozwiązaniu Problemu.

**10.2.1.5    Czas Reakcji**

1. Oznacza czas od Zgłoszenia Problemu do momentu potwierdzenia przez Wykonawcę do Zamawiającego przyjęcia Zgłoszenia Problemu.
2. Wykonawca informuje Zamawiającego o przyjęciu Zgłoszenia Problemu za pośrednictwem poczty elektronicznej lub umieszczeniu odpowiedniej informacji w systemie zgłoszeń problemowych udostępnionym Zamawiającemu.

**10.2.1.6     Rozwiązanie Problemu**

1. W ramach rozwiązywania Problemu, Wykonawca prowadzi diagnostykę, mającą na celu znalezienie przyczyn wystąpienia Problemu. Diagnostyka będzie prowadzona w miejscu instalacji lub zdalnie po wyrażeniu zgody przez Zamawiającego i udostępnieniu Wykonawcy dostępu do Oprogramowania.
2. Wykonawca informuje Zamawiającego o stanie prac mających na celu Rozwiązanie Problemu.
3. W przypadku błędów z Oprogramowaniu Wykonawca procesuje proces poprawy zgodnie z warunkami opisanymi w niniejszym załączniku. W przypadku, gdy Oprogramowanie wymaga re/konfiguracji, będzie ona wykonana przez Wykonawcę.
4. Zamawiający po uzgodnieniu z Wykonawcą, ma prawo zmienić konfigurację we własnym zakresie, następnie przekaże tą informacje Wykonawcy.
5. W przypadku wystąpienia Problemu z Oprogramowaniem, Wykonawca będzie współpracował z producentem Oprogramowania w celu Rozwiązania Problemu.
6. W przypadku wystąpienia Problemu z Oprogramowaniem i wdrożenia ostatecznego Rozwiązania Problemu przy oficjalnym wydaniu nowej wersji Oprogramowania producenta zgodnie z czasami opisanymi w niniejszym załączniku, Wykonawca może zaproponować Obejście w celu Przywrócenia Oprogramowania, opisane w punkcie 10.2.1.8.
7. W przypadku Przywrócenia Oprogramowania poprzez Obejście, Zgłoszenie Problemu zostaje ustawione w odpowiedni stan ze stosowną adnotacją, do momentu ostatecznego Rozwiązania Problemu, zgodnie z czasami określonymi w niniejszym Załączniku.
8. Rozwiązanie Problemu zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt Rozwiązania Problemu, a Zamawiający ten fakt potwierdzi. Zamawiający zostanie poinformowany o fakcie Rozwiązania Problemu za pomocą jednego ze środków komunikacji opisanych w punkcie 8.2.
9. Jeżeli Wykonawca, pięciokrotnie przekroczy terminy usunięcia Problemów, wskazane w niniejszym Załączniku, z przyczyn leżących po jego stronie, Zamawiający będzie miał prawo do usunięcia Problemu na własne ryzyko na koszt Wykonawcy.

**10.2.1.7    Czas Rozwiązania Problemu**

* + - 1. Czas Rozwiązania Problemu liczony jest od momentu Zgłoszenia Problemu do momentu poinformowania Zamawiającego przez Wykonawcę o Rozwiązaniu Problemu.
      2. Czas potwierdzenia przez Zamawiającego do Wykonawcy Rozwiązania Problemu, nie liczy się do Czasu Rozwiązania Problemu – na ten czas Wykonawca zawiesza Zgłoszenie Problemu.
      3. W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku Rozwiązania Problemu tj. dalszego występowania Problemu, Wykonawca odwiesza Zgłoszenie Problemu i Czas Rozwiązania Problemu jest kontynuowany o czas oczekiwania na dostęp do Chmury Prywatnej.

**10.2.1.8    Przywrócenie dostępności Chmury Prywatnej**

1. W ramach rozwiązywania Problemu, Wykonawca może zaproponować Zamawiającemu Przywrócenie Oprogramowania poprzez wykorzystanie Obejścia.
2. Wykonawca informuje Zamawiającego o stanie prac mających na celu Przywrócenie Oprogramowania.
3. Przywrócenie Oprogramowania z wykorzystaniem Obejścia nie zwalnia Wykonawcy z obowiązku Rozwiązania Problemu, zgodnie z czasami określonymi w niniejszym Załączniku.
4. W przypadku wystąpienia Problemu z Chmurą Prywatną, Wykonawca będzie współpracował z producentem Oprogramowania w celu Rozwiązania Problemu.
5. Dla Problemów z Oprogramowaniem, Wykonawca w ramach Przywrócenia Oprogramowania wraz z Zamawiającym instaluje patch, zgodnie z czasami podanymi w niniejszym Załączniku.
6. Przywrócenie Oprogramowania zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt Przywrócenia Chmury Prywatnej, a Zamawiający ten fakt potwierdzi. Zamawiający zostanie poinformowany o fakcie Przywrócenia Chmury Prywatnej za pomocą jednego ze środków komunikacji opisanych w punkcie 8.2.

**10.2.1.9    Czas Przywrócenia Urządzenia**

1. Czas Przywrócenia Chmury Prywatnej mierzony jest oddzielnie dla każdego Zgłoszenia Problemu.
2. Czas Przywrócenia Chmury Prywatnej liczony jest od momentu Zgłoszenia Problemu do momentu poinformowania Zamawiającego przez Wykonawcę o Przywróceniu Oprogramowania.
3. Czas potwierdzenia przez Zamawiającego do Wykonawcy Przywrócenia Chmury Prywatnej, nie liczy się do Czasu Przywrócenia Chmury Prywatnej – na ten czas Wykonawca zawiesza Zgłoszenie Problemu.
4. W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku Przywrócenia Chmury Prywatnej tj. dalszego występowania Problemu, Wykonawca odwiesza Zgłoszenie Problemu i Czas Przywrócenia Chmury Prywatnej jest kontynuowany.
5. W przypadku, gdy w celu Przywrócenia Chmury Prywatnej występuje konieczność instalacji lub naprawy Oprogramowania, na czas instalacji lub naprawy Oprogramowania wymagane jest zastosowanie rozwiązania zastępczego, W przypadku braku takiego rozwiązania, Czas Przywrócenia Chmury Prywatnej odpowiednio wydłuża się o czas oczekiwania na dostęp do Oprogramowania.
6. Zgłoszenie Problemu po Przywróceniu Chmury Prywatnej zostaje ustawione w odpowiedni stan ze stosowną adnotacją, do momentu ostatecznego Rozwiązania Problemu, zgodnie z czasami określonymi w niniejszym załączniku.

**10.2.1.10 Rozwiązanie i zamknięcie Zgłoszenia Problemu**

1. Zgłoszenie Problemu zostaje uznane za rozwiązane w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt Rozwiązania Problemu a Zamawiający ten fakt potwierdzi.
2. Zamawiający zostanie poinformowany o fakcie Rozwiązania Problemu za pomocą jednego ze środków komunikacji opisanych w punkcie 8.2, przy czym Wykonawca jednocześnie dokona stosownej adnotacji w systemie zgłoszeń problemowych.
3. Po potwierdzeniu przez Zamawiającego Rozwiązania Problemu, Wykonawca zamyka Zgłoszenie Problemu w systemie zgłoszeń problemowych.
4. W przypadku analogicznego Zgłoszenia Problemu, zostanie ono zarejestrowane przez Wykonawcę pod innym numerem zgłoszenia.

**10.2.2 Dostarczanie i wsparcie w instalacji Oprogramowania**

W zakresie Gwarancji Wykonawca zapewnia Zamawiającemu usługę dostarczania i wsparcia w instalacji Oprogramowania dla uaktualnień oraz nowych wersji w ramach dostarczonego Oprogramowania.

**10.2.2.1     Dostarczanie Oprogramowania**

* + 1. W okresie Gwarancji Wykonawca będzie udostępniał Zamawiającemu Aktualizacje całego dostarczonego Oprogramowania, oprogramowania SDDC do najnowszych wersji oferowanych przez producenta Oprogramowania (włączając tzw. fixy). Uaktualnienia są realizowane bez ograniczeń ilościowych.
    2. Aktualizacje będą dostarczane Zamawiającemu wraz ze szczegółową procedurą instalacji po przetestowaniu Aktualizacji przez Wykonawcę i potwierdzeniu pozytywnego wyniku testów po stronie Wykonawcy.
    3. Procedura instalacji będzie zawierała również szczegółowe informacje w zakresie wycofania zmian.
    4. W okresie Gwarancji, Wykonawca zapewnia Zamawiającemu dostęp do usług wsparcia technicznego producenta Oprogramowania.

**10.2.2.2     Wsparcie w instalacji Oprogramowania**

* + 1. Wykonawca będzie świadczył Zamawiającemu wsparcie w ramach instalacji Oprogramowania.
    2. Wykonawca może rekomendować, aby instalacja danego Oprogramowania była zrealizowana przez Wykonawcę. W takim przypadku Wykonawca zgłasza taką rekomendację do Zamawiającego, podając uzasadnienie. Zamawiający po konsultacjach z Wykonawcą podejmuje decyzję, czy dane Oprogramowanie zostanie zainstalowane przez Wykonawcę przy asyście Zamawiającego.
    3. Zamawiający może poprosić o procedurę instalacji przetestowaną na urządzeniach testowych celem samodzielnej realizacji.
    4. Wykonawca będzie informował Zamawiającego o krytycznych błędach w oprogramowaniu.
    5. W przypadku, gdy w wyniku instalacji Aktualizacji lub nowej wersji Oprogramowania, pojawi się Problem – zastosowanie mają zapisy z punktu 10.2.1 i podpunktów od 10.2.1.1 do 10.2.1.10

**10.2.2.3    Poziomy świadczenia usługi**

a) Wykonawca gwarantuje następujące poziomy świadczenia usługi

|  |  |
| --- | --- |
|  | Zlecanie Prac |
| Godziny Świadczenia Wsparcia w zakresie Dostarczania instalacji Oprogramowania | W dni robocze 8.00- 17.00 |
| Godziny dla instalacji oprogramowania | Ustalone godziny serwisowe 00:00-24:00 |

**10.2.3 Konsultacje**

W zakresie Gwarancji Wykonawca zapewnia Zamawiającemu usługę Konsultacji.

**10.2.3.1 Przedmiot Konsultacji**

a) W zakresie usługi Konsultacji, Wykonawca zapewnia Zamawiającemu dostęp do pomocy technicznej Wykonawcy jako wsparcie w rozwiązywaniu problemów związanych z bieżącą eksploatacją Chmury Prywatnej, w szczególności w zakresie

* obsługi, administracji i konfiguracji Oprogramowania,
* Integracji, wykonanych zmian,
* wsparcia w rozwiązywaniu problemów u Zamawiającego, które nie są Problemami w rozumieniu niniejszej Umowy,
* Zamawiający szacuje, że będzie korzystał z usługi Konsultacji w sytuacjach szczególnej potrzeby, nie częściej niż kilka razy na kwartał,

b)   Pracownicy pomocy technicznej po stronie Wykonawcy powinni posiadać odpowiednią wiedzę techniczną niezbędną do świadczenia usług konsultacji w ramach Oprogramowania Chmury Prywatnej.

**10.2.3.2 Przebieg Konsultacji**

* + 1. Zamawiający kontaktuje się z Wykonawcą drogą mailową, telefoniczną lub komunikatorem z opisem sytuacji wymagającej Konsultacji.
    2. Wykonawca przekazuje Zamawiającemu potwierdzenie przyjęcia zgłoszenia i rozpoczęcia prac w zakresie danej Konsultacji, zgodnie z czasem podjęcia Konsultacji drogą mailową.
    3. Strony komunikują się wzajemnie w ramach godzin świadczenia Konsultacji w ramach wybranej metody drogą mailową, spotkanie (komunikator online).
    4. Strony dopuszczają zmianę kanału komunikacji na ustalony wspólnie w trybie roboczym.
    5. Wykonawca rejestruje usługi Konsultacji w celach raportowych

**10.2.3.3 Poziomy świadczenia usługi**

a) Wykonawca gwarantuje następujące poziomy świadczenia usługi

|  |  |
| --- | --- |
|  | Zlecanie Prac |
| Czas Podjęcia Konsultacji | 4 godziny robocze |
| Godziny Świadczenia Konsultacji | dni robocze 8.00- 17.00 |

### Raportowanie usług Serwisu Gwarancyjnego

W zakresie Serwisu Gwarancyjnego Wykonawca zapewnia Zamawiającemu dostarczenie raportów z realizacji usługi.

**10.3.1 Termin**

Wykonawca, cyklicznie w trybie trzy miesięcznym (kwartalnym), do 15 Dnia Roboczego kolejnego miesiąca, będzie przekazywał Zamawiającemu za pośrednictwem poczty elektronicznej raporty z realizacji usług Gwarancji w miesiącach ubiegłych.

**10.3.2 Zakres raportu usług diagnostyki i Rozwiązywania Problemów**

W raporcie zostaną uwzględnione, co najmniej następujące dane:

* Numer zgłoszenia,
* Kanał komunikacji,
* Data i godzina rejestracji Zgłoszenia Problemu,
* Określenie zgłaszającego wraz z numerem kontaktowym i adresem poczty elektronicznej,
* Określenie klasyfikacji Problemu,
* Opis Zgłoszenia Problemu,
* Przyczyna wystąpienia Problemu,
* Imię i nazwisko osoby przyjmującej Zgłoszenie Problemu,
* Status zgłoszenia (zamknięte / w trakcie realizacji),
* Czas Reakcji,
* Typ zgłoszenia znacznik tag m.in.: awaria, konfiguracja, zmiana, obszar funkcjonalny,
* Czas Rozwiązania Problemu,
* Czas Przywrócenia Chmury Prywatnej (w przypadku zastosowania Obejścia),
* Sposób Rozwiązania Problemu,
* Sposób Przywrócenia Systemu (w przypadku zastosowania Obejścia),
* Czas poświęcony na realizację danego Zgłoszenia Problemu,
* Zgodność lub brak zgodności z poziomem świadczenia usługi,
* Opis rozwiązania i/lub obejścia,
* Opis podjętych działań celem rozwiązania zgłoszenia.

**10.3.3 Zakres pozostałych raportów**

Szczegółowy zakres pozostałych raportów zostanie uzgodniony przez Strony w trybie roboczym.

**10.3.4. Wykluczenia**

W ramach Gwarancji Wykonawca nie będzie zobowiązany do:

1. Prac realizowanych w lokalizacji Zamawiającego innych niż prowadzących do Rozwiązania.
2. Czynności administracyjnych i konfiguracyjnych innych, niż wynikających z zakresu usług Gwarancji.

**10.3.5 Eskalacje:**

Na wypadek niewykonania przez Wykonawcę lub Zamawiającego zobowiązań wynikających z niniejszego Załącznika w czasie właściwym, Strony ustalą dwa poziomy eskalacji na szczeblu kierownika i dyrektora. Kontakty eskalacyjne oraz forma wymiany informacji zostaną wyznaczone w trybie roboczym.