# Opis przedmiotu zamówienia (OPZ)

Spis treści

[Opis przedmiotu zamówienia (OPZ) 1](#__RefHeading___Toc2955_426739745)

[1. Słownik terminów 2](#__RefHeading___Toc2957_426739745)

[2. Wstęp 6](#__RefHeading___Toc2959_426739745)

[3. Przedmiot zamówienia 7](#__RefHeading___Toc2961_426739745)

[4. Wymagania prawne 7](#__RefHeading___Toc1557_1905956615)

[4.1. Wymagania w zakresie stosowania przepisów prawa. 7](#__RefHeading___Toc1559_1905956615)

[4.2. Wymagania w zakresie serwerów 8](#__RefHeading___Toc2965_426739745)

[4.3. Wymagania w zakresie warstwy przechowywania danych 11](#__RefHeading___Toc2967_426739745)

[4.4. Wymagania w zakresie sieci LAN 12](#__RefHeading___Toc2969_426739745)

[4.5. Wymagania w zakresie sieci WAN 13](#__RefHeading___Toc2973_426739745)

[4.6. Wymagania w zakresie usługi PAM 13](#__RefHeading___Toc2975_426739745)

[4.7. Wymagania w zakresie wsparcia serwisowego elementów infrastruktury 14](#__RefHeading___Toc2977_426739745)

[4.8. Wymagania w zakresie monitoringu infrastruktury 15](#__RefHeading___Toc1561_1905956615_kopia_)

[4.9. Wymagania w zakresie asysty usługi IaaS 15](#__RefHeading___Toc1561_1905956615_kopia1)

[4.10. Wymagania w zakresie bezpieczeństwa 16](#__RefHeading___Toc2981_426739745)

[4.11. Wymagania w zakresie zleceń eksperckich 16](#__RefHeading___Toc2983_426739745)

[4.12. Wymagania w dostawy licencji technologicznych 16](#__RefHeading___Toc1563_1905956615)

[4.13. Wymagania w zakresie inicjalnej konfiguracji i migracji systemów CEIDG i HD 17](#__RefHeading___Toc6573_673195283)

[4.14. Wymagania w zakresie rozbudowy usług 18](#__RefHeading___Toc1563_1905956615_kopia_)

[4.15. Wymagania w zakresie wdrożenia (WD) 19](#__RefHeading___Toc1565_1905956615)

[4.16. Wymagania dotyczące usuwania Awarii (WA) 20](#__RefHeading___Toc2987_426739745)

[4.17. Wymagania w zakresie Disaster Recovery 20](#__RefHeading___Toc1567_1905956615)

[4.18. Wymagania w zakresie zakończenia umowy 21](#__RefHeading___Toc2987_426739745_Copy_1_)

## Słownik terminów

|  |  |
| --- | --- |
| **Termin / skrót** | **Opis** |
| **Zgłoszenie zarejestrowane przez Zamawiającego w systemie SOI** | Zarejestrowanie zgłoszenie w systemie w kategorii:  - awaria  - konsultacja  Awaria to brak możliwości korzystania z usługi przez Użytkowników Systemu z punktu widzenia celów biznesowych. Awaria może być sklasyfikowana jako:   * Błąd Krytyczny, * Błąd Poważny, * Usterka.   Konsultacja - Udzielanie konsultacji przez Wykonawcę polega na zapewnieniu stałej opieki konsultantów, których zadaniem jest pomoc przy rozwiązywaniu bieżących zagadnień związanych z eksploatacją systemu które nie mogą być skategoryzowane jako awaria. |
| **Błąd Krytyczny** | Niepoprawne działanie usługi uniemożliwiające realizację zadań określonych w Ustawie lub dokumentacji technicznej i użytkowej Systemu w zakresie zapewnienia prawidłowego funkcjonowania Systemu, w tym w szczególności brak działania Systemu, zagrożenie dla bezpieczeństwa Systemu lub błędne składowanie danych w bazie Systemu. |
| **Błąd Poważny** | Niepoprawne działanie usługi utrudniające realizację zadań określonych w Ustawie lub dokumentacji technicznej i użytkowej Systemu w zakresie zapewnienia prawidłowego funkcjonowania Systemu. |
| **Usterka** | Każdy inny Błąd nie będącym Błędem Krytycznym Lub Poważnym czyli niepoprawne działanie usługi lub niezgodność funkcjonalności Systemu z warunkami określonymi w Dokumentacji Systemu. |
| **Czas Naprawy** | Czas między zgłoszeniem Awarii, a jej skutecznym i trwałym usunięciem, zgłoszonym przez Wykonawcę. |
| **Czas Reakcji** | Czas między zgłoszeniem Awarii, a uzyskaniem potwierdzenia przystąpienia do jego usunięcia. |
| **Dni Robocze** | Każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej. |
| **Dokumentacja** | Wszelka dokumentacja wytworzona przez Wykonawcę w ramach dostarczenia usługi, dotycząca aspektów technicznych, funkcjonalnych i użytkowych związanych z korzystaniem z Systemów Zamawiającego. |
| **Godziny Robocze** | Godziny od 8:00 do 16:00 w Dni Robocze. |
| **Infrastruktura Chmury Obliczeniowej** | Infrastruktura znajdująca się w dyspozycji Dostawcy Chmury, umożliwiająca dostarczanie przez niego Usług Chmury Obliczeniowej. Infrastruktura znajduje się w minimum dwóch lokalizacjach i z punktu widzenia architektury jest rozproszonym geograficznie klastrem niezawodnościowym HA. |
| **Infrastruktura MRiT** | Wydzielona infrastruktura zlokalizowana w siedzibie Zamawiającego dedykowana dla: Systemu CEIDG (TEST), Hurtowni Danych (TEST) i Biznes.gov.pl (TEST i PROD) - Punktu Informacyjnego dla Przedsiębiorcy oraz systemów pomocniczych (m.in.. backup, monitoring, ITSM) . |
| **Lokalizacja Chmura** | Zarządzana przez Dostawcę Chmury wirtualna platforma widoczna przez Wykonawcę jako zestaw usług typu IaaS i Pass. Z technicznego punktu widzenia jest to klaster HA rozproszony geograficznie (dwie fizyczne lokalizacje) pracujący w trybie "active –active” |
| **Lokalizacja MRiT** | Lokalizacja centrum przetwarzania danych mieszczące się w siedzibie Zamawiającego, dedykowane na potrzeby funkcjonowania CEIDG, Hurtowni danych i Biznes.gov.pl. |
| **Zamawiający (MRiT)** | Ministerstwo Rozwoju i Technologii |
| **Naprawa Awarii** | Trwałe usunięcie Awarii poprzez usunięcie przyczyn powstania Awarii skutkujące przywróceniem pełnej sprawności usługi, w tym również zakończenie innych działań naprawczych. |
| **Obejście Awarii** | Wykonanie tymczasowego sposobu korzystania z innych funkcji lub komponentów usługi, pozwalającego na realizację zadań Zamawiającego określonych w Ustawie lub dokumentacji technicznej i użytkowej Systemu, których normalna realizacja jest utrudniona lub uniemożliwiona z powodu wystąpienia Awarii; zastosowane rozwiązanie nie może powodować utraty lub zmniejszenia funkcjonalności Systemu. |
| **Okno Dostępności** | Czas w ciągu doby poza Oknem Serwisowym. Zamawiający wymaga aby w czasie Okna Dostępności systemy objęte Usługą były w pełni funkcjonalne i dostępne. |
| **Okno Serwisowe** | Czas niedostępności całego systemu lub jego określonych funkcji uzgodniony pomiędzy Zamawiającym a Wykonawcą, przeznaczony na wykonywanie wszelkich niezbędnych prac serwisowych, przeglądów, aktualizacji oprogramowania oraz wgrywania nowych wersji oprogramowania. Okna serwisowe mogą mieć miejsce poza Godzinami Roboczymi. |
| **SLA (Service Level Agreement)** | Poziom dostępności świadczonych usług wyrażony w % w skali okresu rozliczeniowego. |
| **System** | System CEIDG wraz z hurtownią danych i System Biznes.gov.pl. |
| **Umowa** | Umowa zawarta między Zamawiającym, a Wykonawcą wraz ze wszystkimi aneksami i załącznikami do Umowy. |
| **Ustawa** | Ustawa z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy |
| **Użytkownik** | Osoba korzystająca z Systemu lub jego poszczególnych części. |
| **Zgłoszenie** | Przekazanie Wykonawcy zawiadomienia o Awarii lub konsultacji. |
| **WAF** | Web Application Firewall |
| **SNI** | Server Name Identification |
| **System Obsługi Eksploatacji** | System składający się z dwóch systemów:   * Systemu Obsługi Incydentów (SOI) * Systemu Obsługi Zleceń |
| **Mitygacja** | Działania, które mają na celu ograniczanie ryzyka i skutków ataków na usługi Zamawiającego. |
| **System Krytyczny** | System podlegający wymaganiom prawnym wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa oraz jego nowelizacji. |
| **IaaS** | Infrastructure as a Service rozumiana jako infrastruktura chmurowa, która obejmuje nie tylko podstawowe zasoby obliczeniowe i sieciowe oraz pamięć masową, ale także usługi wyższego poziomu , takie jak bazy danych — relacyjne i NoSQL, przetwarzanie danych w czasie rzeczywistym i wsadowe, potoki i usługi dla programistów, kontenery i funkcje. W przeciwieństwie do modelu zakładającego oferowanie „oprogramowania jako usługi” (SaaS), model IaaS nie jest przeznaczony dla typowego użytkownika końcowego. Opracowano go dla działów IT zajmujących się obsługą aplikacji i infrastruktury IT, specjalistów ds. programowania i zarządzania działalnością operacyjną, administratorów systemów i baz danych oraz zaawansowanych programistów. |
| **Maszyna wirtualna** | Maszyna wirtualna to programowa reprezentacja komputera, która emuluje działanie fizycznego komputera lub innego urządzenia. Ma za zadanie udostępnienie środowiska do uruchamiania aplikacji lub systemów operacyjnych, które działają izolowane od fizycznych zasobów sprzętowych. Maszyny wirtualne są stosowane w celu zapewnienia izolacji, zwiększenia bezpieczeństwa, ułatwienia zarządzania zasobami oraz umożliwienia migracji aplikacji pomiędzy różnymi środowiskami sprzętowymi czy operacyjnymi. Przykłady maszyn wirtualnych to VMware, VirtualBox, czy Hyper-V. |
| **Compute VM** | Usługa maszyny wirtualnej z zainstalowanym i działającym systemem operacyjnym w ramach udostępnianej infrastruktury, używana także jako jednostka rozliczenia. |
| **Compute BareMetal** | Compute BareMetal, odnosi się do fizycznego serwera (czyli rzeczywistego, fizycznego urządzenia komputerowego), który działa bezpośrednio na sprzęcie (metal), a nie zwirtualizowany. Oznacza to, że na serwerze BareMetal znajduje się fizyczny procesor, pamięć RAM, dyski twarde oraz inne komponenty sprzętowe, bez żadnej warstwy wirtualizacyjnej. Usługa Compute oznacza, że serwer jest dostarczony ze sprawnym systemem operacyjnym, co umożliwia wykorzystanie pełnych zasobów sprzętowych serwera w sposób bezpośredni. Używana także jako jednostka rozliczenia. |
| **Compute Core** | Rdzeń fizyczny procesora zainstalowanego w serwerze przypisany do usługi Compute VM lub Compute BareMetal. Używany jako jednostka rozliczenia. |
| **Compute RAM** | Wielokość pamięci RAM (Random Access Memory) przypisanej do usługi Compute VM lub Compute BareMetal. Używany jako jednostka rozliczeniowa. |
| **Database as a Service** | Database as a Service (DBaaS) to model dostarczania usług bazodanowych, w którym dostawca usługi zarządza infrastrukturą i oprogramowaniem bazodanowym, zapewniając aplikacjom i użytkownikom dostęp do bazy danych. W tym modelu Zamawiający nie musi zarządzać fizycznymi zasobami ani konfigurować oprogramowania bazodanowego, ponieważ wszystkie te zadania są realizowane przez dostawcę usługi DBaaS. |
| **Backup as a Service** | Backup as a Service (BaaS) to usługa dostarczana przez dostawcę usług., Umożliwiająca tworzenie, zarządzanie i przechowywanie kopii zapasowych danych, aplikacji oraz systemów informatycznych Zamawiającego. Dostawca BaaS odpowiada za procesy tworzenia harmonogramów backupów, zapewnia bezpieczne przechowywanie danych w zdecentralizowanych centrach danych oraz umożliwiają szybkie przywracanie danych w przypadku awarii, minimalizując ryzyko utraty danych i zapewniając organizacjom nieprzerwaną dostępność ich krytycznych informacji. |
| **Tunel VPN** | Tunel VPN (Virtual Private Network) jako usługa w umowie oznacza, że dostawca usług zobowiązuje się do zapewnienia bezpiecznego, zaszyfrowanego połączenia internetowego między urządzeniami Zamawiającego lub partnerów Zamawiającego. |
| **Adres publiczny IPv4** | Adres Publiczny IPv4 jako usługa polega na przydzieleniu unikalnego adresu IP, który umożliwia bezpośredni dostęp do urządzeń w sieci publicznej internetowej. Dostawca tej usługi jest odpowiedzialny za zapewnienie, że adres ten jest unikalny i prawidłowo przypisany.. Ponadto, dostawca musi zapewnić stabilność i dostępność tego adresu, tak aby urządzenia korzystające z niego były zawsze osiągalne z sieci zewnętrznej. W ramach tej usługi dostawca musi zawrzeć monitorowanie i zarządzanie adresem IP, aby zapewnić jego nieprzerwane działanie. |
| **Redundantne łącze symetryczne** | Redundantne łącze symetryczne jako usługa polega na dostarczaniu połączenia internetowego o równej prędkości wysyłania i pobierania danych, z dodatkowym zapasowym łączem w celu zapewnienia ciągłości działania w przypadku awarii głównego łącza. Dostawca tej usługi jest odpowiedzialny za instalację, konfigurację oraz utrzymanie zarówno głównego, jak i zapasowego łącza, aby zagwarantować ich niezawodność i wysoką dostępność. W przypadku awarii głównego łącza dostawca musi zapewnić automatyczne przełączenie na łącze zapasowe bez zakłóceń dla działania systemów Zamawiającego. Dodatkowo, dostawca odpowiada za monitorowania działania łączy, wsparcie techniczne oraz zapewnienia, że zarówno główne, jak i zapasowe łącze spełniają standardy jakości i wydajności. |
| **Storage** | Storage jako usługa chmurowa (Storage as a Service, StaaS) to udostępnianie przestrzeni dyskowej w chmurze, rozliczane na podstawie wykorzystanych gigabajtów (GB) i wybranej klasy wydajnościowej. Dostawca jest odpowiedzialny za zapewnienie wysokiej dostępności i niezawodności usługi, zabezpieczenie danych przed nieautoryzowanym dostępem i utratą, oraz zapewnienie elastyczności i skalowalności przestrzeni dyskowej. Dodatkowo dostawca oferuje wsparcie techniczne i dba o zgodność z przepisami dotyczącymi ochrony danych. Klasy wydajnościowe obejmują standardową wydajność, wysoką wydajność oraz archiwizację, z różnymi cenami zależnymi od wybranego poziomu usług i ilości przechowywanych danych. |
| **Kubernetes as a Service** | Kubernetes as a Service to usługa umożliwiająca zarządzanie klastrami Kubernetes bez konieczności utrzymywania własnej infrastruktury. Dostawca tej usługi jest odpowiedzialny za wdrażanie, monitorowanie oraz utrzymanie całej infrastruktury Kubernetes, zapewniając skalowalność, dostępność i bezpieczeństwo klastrów. Rozliczenie tej usługi odbywa się na podstawie liczby vCore (wirtualnych rdzeni procesora) przypisanych do nodów worker w klastrze Kubernetes, co pozwala na elastyczne dostosowywanie zasobów do potrzeb Zamawiającego. Dostawca zapewnia również wsparcie techniczne, automatyczne aktualizacje, zarządzanie zasobami oraz zgodność z najlepszymi praktykami i standardami branżowymi. |
| **Operator Sekretów** | Operator Sekretów jako usługa to rozwiązanie umożliwiające bezpieczne zarządzanie i przechowywanie danych wrażliwych, takich jak klucze API, hasła czy certyfikaty, w sposób zautomatyzowany. Dostawca tej usługi jest odpowiedzialny za bezpieczne przechowywanie sekretów, zapewniając ich integralność i poufność. Usługa jest rozliczana na podstawie liczby instancji, które są odseparowanymi segmentami zapewniającymi wysoki poziom bezpieczeństwa i izolacji między aplikacjami i środowiskami. Dostawca zapewnia również wsparcie techniczne, automatyczne aktualizacje oraz zgodność z najlepszymi praktykami w zakresie bezpieczeństwa danych. |
| **Usługa DNS** | DNS jako usługa to rozwiązanie umożliwiające zarządzanie systemem nazw domenowych (DNS), które przekłada nazwy domen na adresy IP, ułatwiając komunikację w sieci. Dostawca tej usługi jest odpowiedzialny za zapewnienie niezawodności, dostępności oraz bezpieczeństwa serwerów DNS, jak również za bieżące aktualizacje i monitorowanie systemu. Rozliczanie odbywa się na podstawie instancji, czyli odseparowanych segmentów, które umożliwiają różnym aplikacjom lub środowiskom zarządzanie swoimi konfiguracjami DNS niezależnie. Dzięki temu różne aplikacje lub środowiska nie mogą wzajemnie wprowadzać zmian w konfiguracji, co zapewnia izolację i bezpieczeństwo. Dostawca oferuje także wsparcie techniczne oraz zgodność z najlepszymi praktykami w zakresie zarządzania DNS. |
| **Usługa DHCP** | DHCP jako usługa to rozwiązanie umożliwiające automatyczne przydzielanie adresów IP i innych parametrów sieciowych urządzeniom w sieci. Dostawca tej usługi jest odpowiedzialny za zapewnienie niezawodności, dostępności oraz bezpieczeństwa serwerów DHCP, a także za monitorowanie, utrzymanie i aktualizacje systemu. Usługa jest rozliczana na podstawie instancji, czyli odseparowanych segmentów, które umożliwiają różnym aplikacjom lub środowiskom zarządzanie swoimi konfiguracjami DHCP niezależnie. Dzięki temu różne aplikacje lub środowiska nie mogą wzajemnie wprowadzać zmian w konfiguracji, co gwarantuje izolację i bezpieczeństwo. Dostawca oferuje wsparcie techniczne oraz zgodność z najlepszymi praktykami w zakresie zarządzania DHCP. |
| **System krytyczny** | Systemy krytyczne, zgodnie z polskim prawem, to systemy informacyjne, które mają kluczowe znaczenie dla funkcjonowania państwa i jego instytucji, a także dla ochrony zdrowia, bezpieczeństwa, porządku publicznego oraz stabilności gospodarki narodowej. Awaria lub zakłócenie w działaniu takich systemów może prowadzić do poważnych konsekwencji, w tym zagrożeń dla życia i zdrowia obywateli, utraty poufnych danych, destabilizacji usług publicznych oraz zakłóceń w funkcjonowaniu infrastruktury krytycznej. W związku z tym systemy krytyczne podlegają szczególnym regulacjom prawnym, które określają wymagania dotyczące ich ochrony, zarządzania ryzykiem, ciągłości działania oraz obowiązków informacyjnych i raportowania incydentów bezpieczeństwa. |
| **LoadBalancer** | LoadBalancer jako redundantna usługa to rozwiązanie do równomiernego rozdzielania ruchu sieciowego pomiędzy serwerami, zapewniając wydajność i niezawodność aplikacji. Dostawca jest odpowiedzialny za konfigurację, utrzymanie i monitorowanie usługi oraz jej zabezpieczenia i skalowalność. Usługa jest rozliczana na podstawie instancji, co oznacza odseparowane segmenty, umożliwiające różnym aplikacjom lub środowiskom niezależne zarządzanie konfiguracją bez wzajemnych ingerencji. Dostawca zapewnia ciągłość działania, automatyczne przekierowanie ruchu w przypadku awarii komponentów LoadBalancera, oraz wsparcie techniczne zgodne z najlepszymi praktykami branżowymi. |
| **Usługa CI/CD** | CI/CD jako usługa (Continuous Integration/Continuous Delivery) to zintegrowany zestaw narzędzi wspomagających wytwarzanie oprogramowania. Dostawca tej usługi jest odpowiedzialny za konfigurację, utrzymanie i monitorowanie środowisk CI/CD, które umożliwiają automatyzację procesów budowania, testowania i wdrażania aplikacji. Usługa CI/CD jest rozliczana na podstawie instancji, czyli odseparowanych segmentów, które pozwalają różnym aplikacjom lub środowiskom na niezależne zarządzanie swoimi procesami CI/CD. Dzięki temu zapewniona jest izolacja i bezpieczeństwo, uniemożliwiające wzajemne ingerencje w konfigurację.  Dostawca zapewnia ciągłość działania poprzez monitorowanie stanu usług CI/CD. |
| **Bring your own IP (BYOIP)** | BYOIP (Bring Your Own IP) jako usługa pozwala Zamawiającemu na przeniesienie własnych adresów IP do infrastruktury chmurowej dostawcy. Dostawca tej usługi jest odpowiedzialny za integrację i konfigurację przeniesionych adresów IP w swojej sieci, zapewniając ich prawidłowe działanie i dostępność w środowisku chmurowym |
| **Terraform** | Oprogramowanie Infrastructure-as-a-Code wykorzystwywane przez Zamawiającego. |
| **HPE StoreOnce 3660** | Deduplikator sprzętowy wykorzystywany przez Zamawiającego zainstalowany w lokalizacji MRiT |
| **Commvault Backup & Recovery** | System kopii zapasowych wykorzystywany przez Zamawiającego zainstalowany w lokalizacji MRiT |

## Usługa chmury obliczeniowej na potrzeby systemu teleinformatycznego CEIDG, Hurtowni danych w modelu PaaS oraz na potrzeby systemu Biznes.gov.pl w modelu IaaS.

Dokument ten zawiera szczegółowy opis wymagań dotyczących realizacji usługi udostępnienia infrastruktury IT oraz usług dodatkowych związanych z monitorowaniem i zarządzaniem nią. Przetarg obejmuje szeroki zakres działań, mających na celu zapewnienie wysokiej dostępności, bezpieczeństwa oraz wydajności systemów informatycznych Zamawiającego.

W ramach przetargu planuje się udostępnienie nowej infrastruktury w modelu IaaS w oparciu o usługi chmury obliczeniowej.

W zakres usług wchodzi utrzymanie infrastruktury z proaktywnym wsparciem technicznym, zarządzanie siecią i urządzeniami UTM, monitoring infrastruktury, oraz zarządzanie projektem w systemie zgłoszeniowym Zamawiającego. Przewidziano także usługi asysty technicznej oraz asysty eksperckiej, takie jak wsparcie administracyjne dla aplikacji, systemów operacyjnych i baz danych oraz dostawa niezbędnych licencji technologicznych.

Przedmiot umowy obejmuje dostarczenie przestrzeni chmury obliczeniowej w wyspecjalizowane centra przetwarzania danych, które są przygotowane do obsługi systemów krytycznych. Każde centrum przetwarzania danych musi spełniać następujące kryteria:

1. **Wymogi prawne NIS2**: Centrum musi być zgodne z przepisami dotyczącymi bezpieczeństwa sieci i informacji (NIS2), zapewniając odpowiednią ochronę przed cyber zagrożeniami.
2. **Certyfikat ISO 27001**: Centrum musi posiadać certyfikat ISO 27001, który potwierdza, że zarządzanie bezpieczeństwem informacji spełnia międzynarodowe standardy.
3. **Kryteria TIER III**: Centrum musi spełniać kryteria TIER III według klasyfikacji Uptime Institute, co oznacza zapewnienie wysokiego poziomu dostępności, z możliwością przeprowadzenia konserwacji bez przerw w działaniu usług.

Ponadto, centrum przetwarzania danych musi być wyposażone w odpowiednie mechanizmy ochrony fizycznej i logicznej, w tym redundantne zasilanie, chłodzenie, systemy przeciwpożarowe oraz zaawansowane systemy kontroli dostępu.

Dokument ma na celu precyzyjne określenie wymagań, aby potencjalni wykonawcy mogli przygotować oferty zgodne z oczekiwaniami Zamawiającego, zapewniając tym samym optymalne rozwiązania technologiczne i organizacyjne.

## Przedmiot zamówienia

Przedmiotem umowy jest:

1. Wynajem infrastruktury chmurowej, w tym dedykowanych serwerów i macierzy dyskowych, z gwarancją dostarczenia nowego sprzętu oraz pełnego serwisu technicznego.
2. Wykonanie migracji dwóch systemów zamawiającego Rejestru CEIDG oraz Hurtowni Danych Rejestru CEIDG.
3. Utrzymanie i obsługa techniczna infrastruktury do poziomu IaaS (Infrastructure-as-a-Service), z włączeniem pro-aktywnego wsparcia i zarządzania przez partnera technologicznego.
4. Szeroki zakres usług dodatkowych obejmujący zarządzanie siecią, aktualizacje wszystkich uruchomionych w ramach umowy komponentów infrastruktury, rekonfiguracje oraz integrację z istniejącymi systemami bezpieczeństwa i monitoringu.
5. Dostawa niezbędnych licencji technologicznych.

Oczekuje się, że wybrany dostawca zagwarantuje nie tylko techniczną wydajność, ale również elastyczność operacyjną niezbędną do dostosowania infrastruktury do bieżących i przyszłych wymagań, w tym do planowanego rozbudowania i integracji z nowymi technologiami. Ponadto kluczowe znaczenie będzie miała zdolność dostawcy do współpracy z innymi wykonawcami i dostosowania się do specyficznych wymagań zamawiającego, w tym przepisów dotyczących bezpieczeństwa narodowego (NIS2) oraz ochrony danych.

## Wymagania prawne

### Wymagania w zakresie stosowania przepisów prawa.

Zamawiający wymaga, aby dostarczona usługa była zgodna z regulacjami:

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej: Dz.U. z 2024 r. poz. 422. |
|  | Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne: Dz.U. z 2024 r. poz. 307. |
|  | Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych: Dz. U. 2024 r. poz. 773. |
|  | Ustawa z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy: Dz.U. z 2022 r. poz. 541. |
|  | Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). |
|  | Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną: Dz.U. z 2020 r. poz. 344. |
|  | Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” z późn. zm. |

### Wymagania w zakresie serwerów

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Usługi udostępnione muszą być obsługiwane przez procesory wysokowydajne i elastyczne pod względem konfiguracji, co oznacza dostępność modeli z różną liczbą rdzeni CPU i zróżnicowanym taktowaniem, dostosowanych do różnych obciążeń obliczeniowych. Procesory te powinny pochodzić z serii Intel Xeon Scalable, AMD EPYC lub równoważnej opartej o architekturę x86\_64. Konkretnym wymaganym wynikiem dla udostępnianych procesorów jest osiągnięcie co najmniej 280 punktów w testach w teście SPEC CPU® 2017 Floating Point Rate w konfiguracji dwuprocesorowej. Zamawiający wymaga wraz z ofertą dostarczyć odpowiedni dowód w postaci wydruku pdf z wynikem testu opublikowanego na https://spec.org/cpu2017/results/ zaproponowanego modelu procesora. |
|  | Udostępniona infrastruktura musi oferować elastyczną konfigurację pamięci RAM dla maszyny wirtualnej, umożliwiającą wybór pojemności od kilku GB do 1 TB dla pojedynczej VM. Wsparcie dla pamięci DDR5 musi być zapewnione w najnowszych generacjach maszyn wirtualnych (VM), aby zagwarantować optymalną wydajność i kompatybilność z różnorodnymi obciążeniami roboczymi. |
|  | Udostępniona infrastruktura musi zapewniać wysoką przepustowość sieciową, z możliwością osiągnięcia do 100 Gbps dla maszyn wirtualnych (VM). Ponadto system powinien charakteryzować się niskimi opóźnieniami oraz obsługiwać zaawansowane funkcje sieciowe, takie jak RDMA (Remote Direct Memory Access), w celu zapewnienia wydajnej i niezawodnej komunikacji w wymagających środowiskach obliczeniowych. |
|  | Dodatkowo system musi umożliwiać dodanie zasobów CPU i RAM, bez konieczności restartu maszyny (hot-add). |
|  | System musi gwarantować dostępność na poziomie 99.9% dla każdej VM zgodnie z umową o poziomie świadczenia usług (SLA). |
|  | System musi wykorzystywać mechanizmy odporności na awarię, takie jak Live Migration, w celu minimalizacji przestojów. Dodatkowo system powinien automatycznie przełączać na inne zasoby w przypadku awarii sprzętu, aby zapewnić ciągłość działania i wysoką dostępność usług.  Czas przełączenia maszyny wirtualnej w przypadku awarii któregokolwiek z komponentów jest wliczany w czas niedostępności. |
|  | System musi zapewniać zaawansowane narzędzia monitoringu, do śledzenia kluczowych parametrów wydajnościowych, takich jak obciążenie CPU, zużycie pamięci RAM, przepustowość sieci, stan dysków, dostępność usług oraz zdarzenia związane z bezpieczeństwem. Powinien także oferować konfigurowalne alerty, które reagują na przekroczenie ustalonych progów dla tych parametrów oraz automatyzację reakcji na problemy, aby szybko identyfikować i rozwiązywać nieprawidłowości w działaniu systemu. |
|  | System musi zapewniać izolację i kontrolę dostępu poprzez uwierzytelnianie wieloskładnikowe (MFA) oraz granularne uprawnienia dostępu (RBAC - Role-Based Access Control), aby zagwarantować wysokie bezpieczeństwo i precyzyjną kontrolę nad dostępem do zasobów. |
|  | System musi zapewniać ochronę danych poprzez szyfrowanie danych w spoczynku (Virtual Disk Encryption) oraz w trakcie przesyłu (TLS/SSL), a także obsługę klientów kluczy, w tym możliwość dostarczenia kluczy zarządzanych przez Zamawiającego (External Certificate Authority ) i modułów bezpieczeństwa sprzętowego kontrolowanych przez klientów (Hardware Security Module). |
|  | System musi posiadać zaawansowany moduł audytu i rozliczności tzn.  tworzyć, chronić i przechowywać rejestry audytu systemu informacyjnego w zakresie niezbędnym do umożliwienia monitorowania, analizy, badania i zgłaszania bezprawnych, nieautoryzowanych lub nieodpowiednich działań systemu informacyjnego; oraz (II) zapewnić, aby działania poszczególnych użytkowników systemu informacyjnego mogły być jednoznacznie powiązane z tymi użytkownikami, tak, aby mogli oni zostać pociągnięci do odpowiedzialności za swoje działania. Dostarczony system musi posiadać możliwość eksportu lub udostępnienia danych wszystkich zdarzeń do systemu SIEM Zamawiającego z pojedynczego punktu z którym będzie można wykonać integrację. |
|  | Usługi infrastruktury muszą być oparte o klaster wysokiej dostępności zapewniający wysoką dostępność usług. Klaster świadczący usługi musi spełniać założenie uszkodzenia N+1 tj. przy uszkodzeniu dwóch serwerów będących elementem klastra, zachowuje on możliwość obsługi pełnego obciążenia uruchomionych maszyn wirtualnych. |
|  | Zamawiający wymaga, aby stosunek nad-alokacji zasobów vCPU w klastrze nie przekraczał wartości 2:1 tzn. Ilość dostępnych wątków procesorowych w ramach uruchomionego klastra, nie może być niższa niż dwukrotność przypisanych wirtualnych wątków do procesora dla uruchomionych w klastrze maszyn wirtualnych. Przykład:  Dla klastra posiadającego 192 rdzenie fizyczne procesora ilość przypisanych vCPU do uruchomionych maszyn wirtualnych nie może przekroczyć 386. |
|  | Zamawiający wymaga, aby w ramach usług istniała możliwość uruchomienia serwerów bare-metal w różnych konfiguracjach procesorowych. |
|  | Zamawiający wymaga, aby platforma miała możliwość powołania usługi Kubernetes-as-a-Servce. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi Operatora Sekretów, który posiada co najmniej poniższe funkcjonalności   * Centralne i bezpieczne przechowywanie tokenów, haseł, certyfikatów, kluczy API, par klucz-wartość   Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi LoadBalancera. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi zarządzania tożsamością, która może być zintegrowana z powołanymi w ramach umowy usługami. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi Database as a Service. Usługa musi obsługiwać przynajmniej silniki bazodanowe Microsoft SQL Server Enterprise, MongoDB, Elasticsearch, PostgreSQL, MariaDB, CouchDB. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi Continous Integration/Continous Delivery, w tym co najmniej: repozytorium kodu, usługi weryfikacji bezpieczeństwa i jakości kodu oraz obrazów kontenerowych, repozytorium obrazów kontenerowych. Usługa CI/CD musi być w pełni zintegrowana z platformą i obsługiwać wszystkie inne usługi powołane w ramach umowy. . Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi wewnętrznego serwera DNS, w którym rejestrowane będą wszystkie powoływane usługi. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi wewnętrznego serwera DHCP, w którym rejestrowane będą wszystkie powoływane usługi. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby usługa chmurowa miała możliwość powołania usługi kopii zapasowej na żądanie (Backup as a Service), która ma obejmować wszystkie aspekty uruchomionych usług zarówno pod względem konfiguracji jak i danych przez nie obsługiwanych. |
|  | Zamawiający wymaga, aby wszystkie funkcje API platformy były dokładnie udokumentowane w postaci łatwo dostępnej i interaktywnej platformy. Dostęp do dokumentacji musi być możliwy za pomocą przeglądarki internetowej. Dostęp musi być możliwy z sieci Internet, bez wymogu dodatkowych połączeń VPN, czy dedykowanych tuneli. |

### Wymagania w zakresie warstwy przechowywania danych

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Udostępniona infrastruktura musi oferować różne typy dysków w celu dostosowania do różnych potrzeb wydajnościowych: Ultra SSD zapewniające najwyższą wydajność, niskie opóźnienia, przepustowość do 160,000 IOPS i 2,000 MB/s na dysk; Premium SSD oferujące wysoką wydajność z przepustowością do 20,000 IOPS i 900 MB/s na dysk; Standard SSD zapewniające zbalansowaną wydajność z przepustowością do 10,000 IOPS i 500 MB/s na dysk. Możliwe jest zastosowanie polityk QoS w celu osiągnięcia takiej konfiguracji z tym, że limity tu opisane dotyczą wymogów dla jednego dysku maszyny wirtualnej. |
|  | Udostępniona infrastruktura musi zapewniać skalowalność IOPS (Input/Output Operations Per Second) w zależności od potrzeb aplikacji oraz możliwość konfiguracji i dostosowania IOPS w ramach wybranego typu dysku, aby optymalnie wspierać różnorodne obciążenia robocze. |
|  | Udostępniona infrastruktura musi zapewniać szybki dostęp do danych i minimalizację opóźnień oraz oferować zwiększoną przepustowość dla aplikacji o wysokim zapotrzebowaniu na transfer danych zgodnie z poniższymi klasami, przy czym opóźnienia powinny być mierzone na poziomie urządzenia dyskowego:  **Ultra SSD:**   * 1. Maksymalne opóźnienia: 1 ms   2. Przepustowość: do 2,000 MB/s   **Premium SSD:**   * 1. Maksymalne opóźnienia: 5 ms   2. Przepustowość: do 900 MB/s   **Standard SSD:**   * 1. Maksymalne opóźnienia: 10 ms   2. Przepustowość: do 500 MB/s |
|  | Udostępniona infrastruktura musi również gwarantować dostępność usług storage na poziomie 99,982% usług dysków. Gdzie niedostępnością jest brak dostępu do odczytu lub zapisu danych na dowolnym dysku udostępnionym którejkolwiek maszynie wirtualnej lub usłudze. |
|  | System musi szyfrować dane w spoczynku na macierzy oraz umożliwiać użycie własnych kluczy szyfrowania (Customer-Managed Keys) z możliwością podłączenia modułu bezpieczeństwa sprzętowego (HSM), aby zagwarantować wysokie bezpieczeństwo i kontrolę nad danymi. |
|  | Zamawiający wymaga, aby dostarczona przestrzeń była liczona jako przestrzeń użyteczna tj. dostępna dla serwera lub usługi bez zastosowania mechanizmów deduplikacji oraz kompresji. |
|  | Zamawiający wymaga, aby zamawiana przestrzeń mogła być udostępniona dowolnie i elastycznie do każdej z usług powołanych w ramach usługi chmurowej w postaciach dysków wirtualnych (VM), udziałów S3, PV (Kubernetes), LUN FC (Bare-Metal), NFS, iSCSI. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby w ramach usługi możliwe było uruchomienie maszyny wirtualne opartej o oprogramowanie HPE StoreOnce Virtual Server Appliance w celu synchronizacji kopii zapasowych systemów chmurowych na posiadany przez Zamawiającego fizyczny deduplikator sprzętowy HPE StoreOnce 3660, który znajduje się w Lokalizacji MRiT i jest zarządzany przez administatorów Zamawiającego.,  Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby dostarczona usługa chmurowa była natywne obsługiwana przez posiadane przez Zamawiającego oprogramowania do kopii zapasowych Commvault Backup & Recovery. Oprogramowanie jest zainstalowane w Lokalizacji MRiT i jest zarządzane przez administratorów Zamawiającego. |

### Wymagania w zakresie sieci LAN

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga dostarczenia klastra UTM (Unified Threat Management) z funkcjonalnością zapory sieciowej (FW), którego zadaniem będzie filtrowanie ruchu między strefami DMZ,a aplikacjami oraz filtrowanie ruchu z oraz do Internetu. Klaster UTM musi zapewniać zaawansowane funkcje zabezpieczeń, takie jak wykrywanie i zapobieganie włamaniom (IPS/IDS), filtrowanie treści, inspekcję SSL, ochrona przed malware, kontrola aplikacji oraz zarządzanie regułami dostępu, aby zapewnić kompleksową ochronę sieci.   * Interfejsy sieciowe min. 10 szt * Ilości stref bezpieczeństwa min. 40 * Wydajność mechanizmu FW: min. 20 Gbps * Wydajność mechanizmów Threat Prevention: min 5Gbps * Ilość jednoczesnych sesji (TCP) min. 512 000 * Ilość tunel klienckich IPSec: min 1000 * Redundancja: obsługa HA (Culstering) w trybach: Active/Active i Active/Passive.   Usługa klastra UTM może być realizowana z użyciem usług Virtual Appliance. |
|  | Zamawiający wymaga, aby w ramach usługi chmurowej możliwa była konfiguracja minimum 1000 sieci wirtualnych (vlan), oraz możliwe było konfigurowanie połączeń między nimi. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby w ramach usługi chmurowej połączenia między skonfigurowanymi sieciami wirtualnymi umożliwiały komunikację z prędkością minimum 10Gbps. |
|  | Zamawiający wymaga, aby w ramach usługi chmurowej możliwe było definiowanie tuneli IPsec. Usługa ma pozwalać na zdefiniowanie minimum 100 tuneli IPsec. |
|  | Dostawca musi uruchomić dedykowane łącze punkt-punkt, łącze między lokalizacją Zamawiającego a dostarczaną lokaluzacją Chmury o prędkości 1Gbps, z możliwością rozbudowy do 10Gbps. Ruch na łączu musi zostać dodatkowo zaszyfrowany za pomocą tunelu IPsec. Tunel należy zestawić między routerami posiadanymi przez Zamawiającego, a usługami IPsec dostarczonej usługi chmurowej. Dostawca chmury, może wykorzystać własną istniejącą współdzieloną infrastrukturę chmurową do zaszyfrowania ruchu. |

### 

### Wymagania w zakresie sieci WAN

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby w ramach usługi chmurowej możliwy był dostęp do z sieci Internet symetryczny o przepustowości minimum 1Gbps. Dostęp z internetu musi spełniać SLA na poziomie 99,99. Zamawiający wymaga, aby łącza były zabezpieczone za pomocą usług AntyDDoS. Niedostępność usługi ze względu na trwający atak jest traktowana jako zwykła niedostępność usługi. |
|  | Zamawiający wymaga, aby w ramach usługi chmurowej możliwa była konfiguracja adresów publicznych IP oraz ich podłączenie do dowolnej z uruchomionych usług. Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury. |
|  | Zamawiający wymaga, aby w ramach usługi było możliwe uruchomienie własnej. adresacji publicznej, której jest właścicielem na zasadzie BYOIP (Bring Your Own IP)  Powołanie wraz z konfiguracją zasobu musi być w pełni zautomatyzowane i możliwe za pośrednictwem API oraz pakietu Terraform dostarczonego przez producenta lub dostawcę chmury.  Usługa BYOIP jest rozliczana na podstawie liczby podsieci zainstalowanych w usłudze chmurowej. Dostawca musi zapewnić, że każda podsieć jest odpowiednio izolowana, co gwarantuje bezpieczeństwo i zapobiega konfliktom adresów IP między różnymi użytkownikami. Ponadto, dostawca jest odpowiedzialny za zarządzanie routingu, monitorowanie wydajności oraz utrzymanie dostępności usług powiązanych z przeniesionymi adresami IP.  Dostawca odpowiada również za wsparcie techniczne, pomagając Zamawiającemu w konfiguracji i zarządzaniu ich adresami IP w chmurze, oraz dba o zgodność usługi z najlepszymi praktykami i standardami branżowymi, aby zapewnić najwyższą jakość i bezpieczeństwo. |

### Wymagania w zakresie usługi PAM

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby w ramach usługi chmurowej został dostarczony system PAM (Privileged Access Management), którego celem jest nagrywanie użytkowników z uprawnieniami administracyjnymi wykonującymi zmiany w aplikacjach i systemach Zamawiającego uruchomionych na udostępnionej infrastrukturze. |
|  | Zamawiający wymaga przechowywania nagrań przez 12 miesięcy. |
|  | Zamawiający wymaga dostępu do podglądu pracy administratora Systemu oraz możliwości pobrania pliku nagrania sesji w formacie mp4 bezpośrednio z dashboardu systemu. |
|  | System PAM musi umożliwiać działanie w trybie transparentnym, proxy lub bastion. |
|  | System PAM musi wspierać uwierzytelnianie wieloskładnikowe (MFA). Zamawiający wymaga wysokiej jakości wsparcia dla portokołów SSH i RDP w tym obsługi protokołów X11, SSH-AGENT, SCP, SFTP, Device Redirection, TSCLIENT |
|  | Zamawiający wymaga, aby dostarczony system był objęty aktywnym kontraktem serwisowym. |
|  | Zamawiający wymaga, aby dostarczony system był proaktywnie aktualizowany zgodnie z zaleceniami producenta. System powinien być aktualizowany nie rzadziej niż raz na 3 miesiące. |
|  | Zamawiający wymaga, aby system PAM obsługiwał OCR sesji umożliwiający pełne wyszukiwanie kontekstowe dla wybranych użytkowników lub serwerów wskazanych przez Zamawiającego |
|  | Zamawiający wymaga, aby system był w stanie obsłużyć do 350 serwerów oraz umożliwiał pracę dla minimum 35 połączeń jednocześnie, nie powodując obniżenia wydajności. |
|  | Zamawiający wymaga, aby inicjalnie dostarczyć system PAM umożliwiający podłączenie do 65 serwerów. Rozbudowa do 300 serwerów nastąpi na żądanie Zamawiającego nie później niż 30 dni od daty złożenia zamówienia. |
|  | Zamawiający wymaga, aby opłata za użytkowanie systemu rosła dynamicznie wraz z zamówioną pojemnością. Minimum 65 serwerów, maksymalnie 300 serwerów podpiętych do PAM. |
|  | Zamawiający wymaga przekazywania cyklicznie nagrań na udostępnionych przez Zamawiającego nośnikach (dyski HDD/SSD na USB) |

### Wymagania w zakresie wsparcia serwisowego elementów infrastruktury

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby dostawca zapewnił pełne wsparcie techniczne i serwisowe, w tym szybką reakcję na zgłoszenia, regularne aktualizacje oprogramowania oraz doradztwo w zakresie najlepszych praktyk bezpieczeństwa w ramach dostarczonego rozwiązania. |
|  | Dostawca musi zapewnić dedykowany zespół wsparcia, który będzie dostępny 24/7 do reagowania na zgłoszenia i rozwiązywania problemów. Zespół ten musi posiadać wysokie kwalifikacje i doświadczenie w zakresie konfiguracji i naprawy dostarczonych usług infrastruktury. |
|  | Dostawca musi przeprowadzać regularne aktualizacje oprogramowania udostępnionej infrastruktury, w tym łatki bezpieczeństwa, aby system był zawsze zabezpieczony przed najnowszymi zagrożeniami. |
|  | Dostawca musi zorganizować i przeprowadzić warsztaty dla personelu IT Zamawiającego, mających na celu podniesienie świadomości i kompetencji w zakresie obsługi i zarządzania usługami chmury. Warsztaty będą prowadzone na zlecenie Zamawiającego. Nie częściej niż cztery razy w danym roku kalendarzowym. Warsztaty powinny zostać przeprowadzone w formie online z możliwością ich rejestracji i udostępnienia w formie wideo. Warsztaty będą prowadzone dla maksymalnie 5 administratorów Zamawiającego. Powinny trwać nie krócej niż 8 godzin lekcyjnych (8x 45 min) |
|  | W przypadku stwierdzenia incydentu bezpieczeństwa Zamawiający wymaga, aby Wykonawca przeprowadził pełną analizę bezpieczeństwa w zarządzanym przez siebie obszarze, wynikiem czego musi być raport zawierający pełną analizę oraz argumentację potwierdzoną dowodami. |

### Wymagania w zakresie monitoringu infrastruktury

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga uruchomienia systemu monitorowania elementów udostępnionej infrastruktury. |
|  | Dostarczone usługi monitorowania, mogą składać się z wielu elementów realizujących zadanie w całości. |
|  | Zamawiający wymaga, aby monitorowaniu podlegały wszystkie elementy udostępnionej infrastruktury. |
|  | Zamawiający wymaga dostępu w trybie read-only do wszystkich komponentów składających się na usługę monitorowania. |
|  | Zamawiający wymaga, aby system monitorowania generował powiadomienia o zdarzeniach i przesyłał je w wielu kanałach. Minimum e-mail, udostępniony dashboard, powiadomienie sms/Signal |

### Wymagania w zakresie asysty usługi IaaS

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby Zespół dostawcy na podstawie zlecenia asysty infrastruktury wykonywał konfiguracje i powoływanie zasobów na udostępnionej infrastrukturze. |
|  | Zamawiający wymaga, aby zespół Dostawcy pro aktywnie wskazywał miejsca i elementy wymagające dodatkowej konfiguracji, bądź aktualizacji w celu zwiększenia bezpieczeństwa bądź niezawodności aplikacji uruchomionych przez Zamawiającego. |
|  | Zamawiający wymaga, aby zespół Dostawcy konfigurował systemy operacyjne, bądź jego komponenty na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby zespół dostawcy konfigurował systemy i silniki baz danych jak i wewnętrzne komponenty silnika na zlecenie Zamawiającego |
|  | Zamawiający wymaga, aby zespół dostawcy konfigurował wszystkie inne komponenty dostarczonej infrastruktury na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby zespół dostawcy konfigurował kopie zapasowe komponentów dostarczonej infrastruktury na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby zespół dostawcy tworzył mechanizmy automatyzacji zadań konfiguracji infrastruktury na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby zespół dostawcy tworzył i udostępniał dodatkowe parametry oraz dashboardy w ramach systemu monitoringu na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby wszystkie konfiguracje były wykonywane za pomocą narzędzia Infrastructure as a Code tj. Terraform,Ansible i metodyki GitOps. Kod będzie uruchamiany w ramach dostarczonej infrastruktury. Aktualny kod konfiguracji infrastruktury będzie udostępniany Zamawiającemu wraz z przekazaniem praw autorskich do niego. Wszystkie wykorzystane narzędzia muszą zostać zaakceptowane przez Zamawiającego oraz musi on posiadać odpowiednie prawa do korzystania z nich w ramach udostępnionej infrastruktury. |
|  | Dostawca może wykonać prace bez wykorzystania narzędzi Infrastructure as a Code tylko w uzasadnionych przypadkach i po uzyskaniu zgody Zamawiającego. |
|  | Zamawiający wymaga, aby zespół dostawcy tworzył dokumentacje i instrukcje poszczególnych aspektów działania infrastruktury na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby rozliczanie usług asysty infrastruktury odbywało się na podstawie zleceń w systemie zgłoszeniowym Zamawiającego. |

### Wymagania w zakresie bezpieczeństwa

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Oczekuje się, że dostawca przeprowadzi kompleksowe testowanie i walidację systemu przed jego pełnym wdrożeniem, aby upewnić się, że wszystkie wymagania techniczne są spełnione. |
|  | Dostawca musi przeprowadzić zarówno testy funkcjonalne (sprawdzające, czy system działa zgodnie z oczekiwaniami i wymaganiami), jak i niefunkcjonalne (oceniające aspekty takie jak wydajność, bezpieczeństwo, skalowalność). |
|  | Dostawca musi potwierdzić, czy system jest zgodny z międzynarodowymi standardami i praktykami bezpieczeństwa, takimi jak OWASP, ISO/IEC 27001, GDPR. |
|  | Dostawca w ramach testów musi zweryfikować mechanizmy redundancji i ciągłości działania, w tym testowanie automatycznego przełączania i systemów zapasowych. |
|  | Dokładne dokumentowanie wyników wszystkich testów, w tym zidentyfikowanych problemów i sposobów ich rozwiązania. Zamawiający wymaga, aby dokumenty zostały dostarczone w ramach zakończenia wdrożenia. |

### Wymagania w zakresie zleceń eksperckich

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby zespół Dostawcy na podstawie zleceń eksperckich świadczył usługi zaawansowanej analizy architektury, technologii oraz wsparcia w zarządzaniu danymi i usługami uruchomionymi w ramach udostępnionej infrastruktury chmurowej. |
|  | Zamawiający wymaga, aby zespół Dostawcy realizował zadania w zakresie optymalizacji baz danych, analizy błędów konfiguracyjnych, wykonywał upgrade stosu technologii wraz z migracją danych, projektował i wdrażał rozwiązania poprawiające bezpieczeństwo i stabilność systemów bazodanowych na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby zespół Dostawcy realizował zadania w zakresie optymalizacji i zaawansowanej konfiguracji systemów operacyjnych wraz z ich komponentami, wykonywał upgrade wraz z migracją danych, projektował i wdrażał rozwiązania poprawiające bezpieczeństwo i stabilność systemów operacyjnych na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby zespół Dostawcy realizował zadania w zakresie optymalizacji procesów DevOps, projektował i wdrażał procesy poprawiające bezpieczeństwo i stabilność systemów bazodanowych na zlecenie Zamawiającego. |
|  | Zamawiający wymaga, aby rozliczanie usług zleceń eksperckich odbywało się na podstawie zleceń w systemie zgłoszeniowym Zamawiającego. |

### Wymagania w dostawy licencji technologicznych

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga dostarczenia licencji systemu operacyjnego Windows Server Datacenter w wersji 2022 w liczbie umożliwiającej zalicencjonowanie 144 rdzeni fizycznych wraz z pełnym wsparciem producenta i pakietem SoftwareAssurance na okres 36 miesięcy. Licencja ma zostać dostarczona nie później niż 30 dni od podpisania umowy. |
|  | Zamawiający wymaga dostarczenia licencji baz danych SQL Server Enterprise 2022 umożliwiających zalicencjonowanie 32 rdzeni fizycznych wraz z pełnym wsparciem producenta i pakietem SoftwareAssurance na okres 36 miesięcy. Licencja ma zostać dostarczona nie później niż 30 dni od podpisania umowy. |
|  | Zamawiający dopuszcza dostarczenie licencji w formie subskrypcji, natomiast przy takiej formie muszą one zostać dostarczona na okres minimum 72 miesięcy. |
|  | Zamawiający wymaga dostarczenia licencji HPE StoreOnce VSA 32TB wraz z pełnym w wsparciem producenta na okres 36 miesięcy. Licencja ma zostać dostarczona nie później niż 30 dni od zgłoszenia takiej potrzeby przez Zamawiającego. |

### Wymagania w zakresie inicjalnej konfiguracji i migracji systemów CEIDG i HD

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć 60 sztuki Compute VM. Klaster obsługujący powyższe VM musi być zgodny z licencjonownowaniem Microsoft Windows Server 2022 Datacenter w ilości dostarczanej w ramach **WWL-2** |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć 4 sztuki Compute BareMetal. Klaster musi być zgodny z licencjonowaniem Microsoft Windows Server 2022 Standard oraz Microsoft SQL Server Enterprise 2022 w ilości dostarczanej w ramach **WWL-2 oraz WWL-3** |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć 250 sztuk Core, które będą przypisane do wyżej wymienionych Compute VM oraz Compute BareMetal |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć usługę 3072 GB RAM, które będą przypisane do wyżej wymienionych Compute VM oraz Compute BareMetal |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć usługę 25 TB Storage – Ultra SSD, które będą przypisane do wyżej wymienionych Compute BareMetal |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć usługę 25 TB Storage – Premium SSD, które będą przypisane do wyżej wymienionych Compute VM |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć usługę 4 instancje DBaaS MSSQL, które będą uruchomione w ramach wyżej wymienionych Compute BareMetal. |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej zestawić 8 tuneli IPsec. Zestawienie tuneli zostanie skoordynowane przez Zamawiającego. |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej uruchomił usługę Backup as a Service dla 50TB przestrzeni. |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć łącze symetryczne Internet o przepustowości 1Gbps |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczyć 32 publiczne adresy IPv4 |
|  | Zamawiający wymaga, aby w ramach inicjalnego uruchomienia usługi chmurowej dostarczył łącze symetryczne punkt-punkt między lokalizacją MRiT oraz lokalizacją Chmurową. |
|  | Zamawiający wymaga, aby w ramach migracji systemów CEIDG i HD Dostawca dokonał migracji maszyn wirtualnych oraz baz danych na nowe środowisko. |
|  | Aktualne środowisko jest oparte o infrastrukturę VMware ESXi 6.7 i zbudowane na bazie maszyn wirtualnych. Szczegółowy opis w załącznikach. |
|  | W ramach przygotowania do migracji dostawca opracuje z Zamawiającym szczegółowy plan migracji z uwzględnieniem koniecznych przerw technologicznych. |
|  | Zamawiający zapewni wsparcie na poziomie aplikacji, dostawca będzie odpowiedzialny za migrację na warstwie infrastruktury, systemów operacyjnych i baz danych. |

### Wymagania w zakresie rozbudowy usług

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 350 sztuk maszyn wirtualnych (Compute VM). |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 8 sztuk serwerów fizycznych (Compute BareMetal). |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 1500 rdzeni fizycznych przypisanych w ramach maszyn wirtualnych i serwerów fizycznych. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 12 TB pamięci RAM przypisanych w ramach maszyn wirtualnych i serwerów fizycznych. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 16 instancji MS SQL Enterprise rozlokowanych w ramach maszyn wirtualnych i serwerów fizycznych. Licencje zostaną dostarczone przez Zamwiającego. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 400TB usługi Backup as a Service. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 20 sztuk Tuneli VPN. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację do 128 sztuk adresów publicznych IPv4 dostępnych w ramach łącza symetrycznegi (Internet). |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację łącza symetrycznego (Internet) do przepustowości 10Gbps. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację łącza symetrycznego (DC-PTK) do przepustowości 10Gbps. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację Storage- Ultra SSD do 50 TB przestrzeni użytecznej. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację Storage – Premium SSD do 100 TB przestrzeni użytecznej. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację o usługi Database as a Service (OpenSource) do 80 instancji. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację o usługi Operatora Sekretów do 8 instancji. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację o usługi lokalnego serwera DNS do 8 instancji. |
|  | Zamawiający wymaga, aby w ramach usług można było rozbudować inicjalną konfigurację o usługi lokalnego serwera DHCP do 8 instancji. |

### Wymagania w zakresie wdrożenia (WD)

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby w ramach oferty dostarczony został harmonogram ramowy zawierający główne etapy i kamienie milowe przedstawione na osi czasu. |
|  | Zamawiający wymaga, aby wykonawca dostarczył i ustalił harmonogram szczegółowy w ciągu 14 dni od podpisania umowy. Dostarczony harmonogram podlega akceptacji Zamawiającego. Dokument musi zawierać szczegółową listę zadań, dokładne daty rozpoczęcia i zakończenia każdego zadania. Dokładnie regulować zależności i odpowiedzialności pomiędzy zadaniami. Wykonawca opracuje harmonogram szczegółowy na podstawie analizy dokumentacji i aktualnej konfiguracji dostarczonej przez Zamawiającego. Możliwe jest też ustalenie warsztatów wraz z zespołem Zamawiającego oraz jego podwykonawcami w razie zgłoszonej potrzeby. Harmonogram szczegółowy ma zawierać wszystkie prace projektowe w zakresie punktów WD 3 do WD 6 wraz z ujęciem okresu utrzymania całości dostarczonych komponentów poprzez czas trwania umowy. |
|  | Zamawiający wymaga, aby Dostawca w ciągu 30 dni od podpisania umowy uruchomił i skonfigurował środowisko dla dwóch aplikacji Zamawiającego tj. Rejestru CEIDG i Hurtowni Danych. Szczegóły konfiguracyjne zostaną ujęte w harmonogramie szczegółowym. |
|  | Zamawiający wymaga, aby Dostawca przeniósł, odtworzył dane i uruchomił produkcyjnie systemy Rejestru CEIDG i Hurtowni Danych w ciągu 60 dni od podpisania umowy we współpracy z Zamawiającym. |
|  | Zamawiający wymaga, aby wykonawca 1 dzień przed końcem realizacji punktu WD 4 dostarczył dokumentację zawierającą szczegółowe informacje techniczne dotyczące projektu, w tym wymagania, standardy i parametry techniczne. Dokumentacja dodatkowo ma uwzględniać graficzne przedstawienia projektu, takie jak schematy, plany, rysunki konstrukcyjne, diagramy blokowe. Procedury i wytyczne dotyczące użytkowania, utrzymania i rozwoju systemu. Wykonawca przed jej dostarczeniem ustali z Zamawiającym szczegółowy kształt i format dokumentacji. |
|  | Zamawiający wymaga, aby wykonawca 1 dzień przed końcem realizacji punktu WD 4 dostarczył usługę systemu monitoringu opisany w punkcie 4.8. Wykonawca przed jej dostarczeniem ustali z Zamawiającym szczegółowy kształt i format dashboardów oraz kanałów powiadamiania o wykrytych zdarzeniach. |
|  | Zamawiający wymaga, aby Wykonawca uwzględnił aktualizację dokumentacji w harmonogramie szczegółowym i związany z nimi czas na minimum 2 iteracje. |
|  | Zamawiający wymaga, aby wykonawca 45 dni od uruchomienia systemów produkcyjnie środowisku produkcyjnym wykonał testy i walidacje opisane w sekcji WT 9 oraz dostarczył raporty z ich wykonania do wglądu Zamawiającego. |
|  | Systemu Obsługi Incydentów udostępniony i administrowany przez Zamawiającego, umożliwiającego rejestrację zgłoszeń oraz nadzorowanie procesu usuwania Awarii. |
|  | System obsługi incydentów – reguły rejestracji zgłoszenia:   1. skorzystanie z elektronicznej usługi SOI, a w przypadku niedostępności 2. wysłanie wiadomości elektronicznej przesłanej na adres …………………., 3. lub pisma przesłanego na adres ………………………….., 4. lub telefonicznie pod numerem telefonu …………………., przy czym Zgłoszenie takie wymaga niezwłocznego potwierdzenia w jednej z form wskazanych w pkt a) lub b). |
|  | Korzystanie z kanałów komunikacji opisanych w WD 9 od b) do d) dopuszcza się w przypadku braku możliwości dokonania Zgłoszenia za pomocą Elektronicznej usługi SOI. Z chwilą przywrócenia tej możliwości Wykonawca niezwłocznie uzupełnia Zgłoszenia w ww. systemie i wszystkie komunikaty zwrotne. |

### Wymagania dotyczące usuwania Awarii (WA)

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zgłoszenia Awarii będą dokonywane za pośrednictwem SOI przez upoważnionych pracowników Wykonawcy oraz Zamawiającego. Zamawiający zobowiązany jest przekazać Wykonawcy w terminie 1 tygodnia od dnia zawarcia Umowy listę upoważnionych pracowników Zamawiającego. Zmiana osób wskazanych w ww. liście następuje poprzez pisemne powiadomienie Wykonawcy bez konieczności podpisywania aneksu do Umowy. |
|  | Jeżeli Awaria została wykryta przez pracowników Wykonawcy lub Wykonawca otrzymał informację o wystąpieniu Awarii z dowolnego zewnętrznego źródła, obowiązkiem Wykonawcy jest niezwłocznie przystąpienie do usuwania Awarii oraz poinformowanie Zamawiającego o wystąpieniu Awarii oraz zarejestrowanie Awarii w SOI w czasie nie dłuższym niż 0,5 godziny. |
|  | Przyjmuje się, że Zgłoszenie Usunięcia Awarii rozpoczyna się z chwilą zarejestrowania Awarii w SOI. |
|  | Zamawiający ma prawo do zgłaszania Awarii przez cały rok, 7 dni w tygodniu, 24 godziny na dobę. Czas na usunięcie Awarii rozpoczyna się w momencie Zgłoszenia Usunięcia Awarii. |
|  | Jeśli dla dokonania usunięcia Awarii obiektywnie niezbędne będzie podjęcie przez Zamawiającego określonych czynności lub przekazanie dodatkowych wyjaśnień Wykonawca może się zwrócić do Zamawiającego. Czas na udzielanie wyjaśnień nie będzie wliczany do czasu obsługi Zgłoszenia Usunięcia Awarii. Przy obsłudze złożonych Awarii Zamawiający może zdecydować o wielokrotnym zadawaniu pytań i udzielaniu odpowiedzi przez Zamawiającego. |
|  | Informację o usunięciu Awarii Wykonawca będzie zgłaszał w Systemie Obsługi Incydentów . |
|  | O zakończeniu usunięcia Awarii decyduje Zamawiający. |
|  | Skuteczne usunięcie Awarii Zamawiający będzie potwierdzał w Systemie Obsługi Incydentów. |
|  | Jeżeli Wykonawca nie dokona naprawy w terminach, wskazanych w Tabeli 1 umieszczonej poniżej, Zamawiający może:   1. obciążyć Wykonawcę karą umowną na zasadach opisanych w Umowie, 2. zawiadamiając uprzednio Wykonawcę, usunąć Awarię we własnym zakresie lub powierzyć jej usunięcie innemu podmiotowi trzeciemu na koszt Wykonawcy. Naprawa nie powoduje wygaśnięcia oraz utraty jakichkolwiek praw wynikających z tytułu gwarancji.. |

Tabela 1 Wartości Czasów Naprawy (od czasu Rejestracji Zgłoszenia)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Błąd Krytyczny  (godziny)** | **Błąd Poważny  (godziny)** | **Usterka  (godziny)** |
| 1 | Czas Reakcji | 0,5 | 0,5 | 0,5 |
| 2 | Czas zastosowania Obejścia | 0,5 | 1 | nie dotyczy |
| 3 | Czas Naprawy | 1 | 2 | 24 |

### Wymagania w zakresie Disaster Recovery

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający wymaga, aby Dostawca w ramach udostępnionej infrastruktury opracował wraz z Zamawiającym procedurę Disaster Recovery obejmującą kompletną niedostępność usług świadczonych przez Dostawcę i konieczność odtworzenia systemu na infrastrukturze w lokalizacji MRiT. |
|  | Zamawiający wymaga, aby Dostawca przekazywał pełną kopię zapasową wykonywaną w ramach usług na nośnik udostępniony przez Zamawiającego wraz z procedurą odtworzenia zawartych na nim danych. Format przekazanych musi być zostać uzgodniony z Zamawiającym. Przekazane dane wraz z procedurą muszą umożliwić odtworzenie danych z użyciem technologii VMware ESXi w wersji 7 lub wyższej oraz oprogramownaia Commvault Backup & Recovery. |
|  | Zamawiający wymaga, aby Dostawca dokonywał przeglądu oraz testów symulacyjnych procedury Disaster Recovery nie rzadziej niż raz na rok i sporządzał z tego tytułu raport. |
|  | Zamawiający wymaga, aby dane dostępowe będące w posiadaniu Dostawcy do systemu w szczególności hasła użytkowników standardowych takich jak root czy administrator były przekazywane wraz z kopią zapasową, oddzielnym kanałem na szyfrowanym nośniku. Zakres oraz listę wymaganych do przekazania haseł Dostawca uzgodni wraz z Zamawiającym. |

### Wymagania w zakresie zakończenia umowy

|  |  |
| --- | --- |
| **Numer wymagania** | **Opis wymagania** |
|  | Zamawiający, wymaga aby Dostawca umożliwił, dokonał wszelkich starań i wsparł proces wyjścia systemu na nową infrastrukturę na koniec obowiązywania umowy z minimalizacją czasu niedostępności systemu. |
|  | Zamawiający, wymaga aby wszelkie Dane pozostałe na urządzeniach udostępnionych Zamawiającemu zostały w zamazane lub zniszczone w taki sposób, że niemożliwe jest ich odtworzenie. Z tego procesu zostanie sporządzony i dostarczony odpowiedni protokół zniszczenia danych. |