

Numer sprawy: OR-D-III.272.90.2022.AS

Załącznik nr 2 do specyfikacji warunków zamówienia

Opis Przedmiotu Zamówienia

Na „*Usługę zapewnienia infrastruktury teleinformatycznej w modelu chmurowym oraz projekt i budowę sieci WAN*” w ramach projektów: „*Informatyzacja bibliotek pedagogicznych na Mazowszu*” oraz „*Regionalna Platforma Informacyjna – Kultura na Mazowszu*”.

Spis treści

1. Zakres realizacji prac	3
2. Opracowanie dokumentu pn. Projekt techniczny Infrastruktury	3
3. Wymagania dla infrastruktury chmurowej	4
4. Wymagania dla sieci WAN.....	8
5. Przeprowadzenie instruktaży dla Zamawiającego	8
6. Dokumentacja powykonawcza.....	9
7. Warunki równoważności oprogramowania	10

1. Zakres realizacji prac

Przedmiotem zamówienia jest świadczenie usługi dostarczania zasobów informatycznych w postaci chmury obliczeniowej dla systemów MBP i MPK oraz stworzenie i utrzymanie sieci WAN. W ramach świadczonej usługi Wykonawca:

- 1) opracuje i uzgodni z Zamawiającym szczegóły projektu technicznego świadczonej usługi chmurowej oraz sieci WAN, zgodnie z wymaganiami Rozdziału 2. Opracowanie dokumentu pn. Projekt techniczny Infrastruktury,
- 2) uruchomi usługę chmurową oraz komunikację (sieć WAN) infrastruktury zlokalizowanej w chmurze z siedzibami Partnerów projektu i Zamawiającego zgodnie z wymaganiami Rozdziału 3. Wymagania dla infrastruktury chmurowej, Rozdziału 4. Wymagania dla sieci WAN oraz dokumentem pn. Projekt techniczny Infrastruktury,
- 3) będzie utrzymywał usługę chmurową oraz sieć WAN w ciągłości działania,
- 4) będzie zapewniał odporność cybernetyczną,
- 5) będzie zapewniał obsługi kopii zapasowych, odtwarzania oraz obsługi klasy disaster recovery,
- 6) będzie zapewniał utrzymanie wymaganych parametrów przez cały okres pracy Systemu.

2. Opracowanie dokumentu pn. Projekt techniczny Infrastruktury

- 1) W skład Projektu Technicznego infrastruktury wchodzi:
 - a) projekt techniczny sieci WAN,
 - b) wytyczne, wzorcowe konfiguracje, opisy zasad oraz politykę bezpieczeństwa usługi chmurowej, które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji,
 - c) opis stosowanych mechanizmów zapewnienie bezpieczeństwa,
 - d) opis mechanizmów wykonywania i odtwarzania kopii zapasowych maszyn oraz konfiguracji uruchomionej w ramach usługi chmurowej,
 - e) opis mechanizmu przejmowania działania przez zapasowe środowisko przetwarzania danych (Disaster Recovery Center),
 - f) opis mechanizmów uruchomienia maszyn wirtualnych w oparciu o predefiniowany szablon z systemem operacyjnym oraz zaimportowany plik *.vhd,
 - g) opis mechanizmu zarządzania maszynami wirtualnymi,
 - h) opis procedury przydzielenia Operatorom dostępów do wirtualnych maszyn,
 - i) opis procedur i zasad zarządzania użytkownikami przez Administratorów,
 - j) opis mechanizmu tworzenia, konfiguracji i zarządzania sieciami VLAN w chmurze,
 - k) opis mechanizmu tworzenia dostępów do maszyn wirtualnych i uruchomionych usług,
 - l) opis mechanizmu udostępniania usług w sieci Internet,
 - m) opis mechanizmów komunikacji pomiędzy chmurą a Punktami Odbioru Usługi za pośrednictwem sieci WAN,
 - n) plan testów poprawności działania i bezpieczeństwa usługi chmurowej oraz sieci WAN,

- o) scenariusze testowe w zakresie poprawności konfiguracji usługi chmurowej oraz sieci WAN,
 - p) wzór Raportu z testów działania usługi zapewnienia zasobów chmurowych oraz Raportu działania sieci WAN, zgodnych z planem testów i scenariuszami testowymi o których mowa w pkt n) oraz o),
 - q) opis procedury i mechanizmu usuwania/migracji danych Zamawiającego.
- 2) Projektowana infrastruktura musi zapewniać możliwość wprowadzania zmian w konfiguracji oprogramowania i infrastrukturze z zachowaniem ciągłości pracy całego systemu.
 - 3) W Projekcie technicznym sieci WAN musi być zawarty logiczny podział na projekty e-kultura oraz e-biblioteki, sieci WAN dla Partnerów poszczególnych projektów muszą być odseparowane, zgodnie z Załącznikiem nr 5 do Umowy „Wykaz Punktów Odbioru Usługi”,
 - 4) Dokument, o którym mowa w ust. 1), podlega odbiorowi przez Zamawiającego.
 - 5) Dokument, o którym mowa w ust. 1), musi zostać napisany w języku polskim, zgodnie z dokumentem „Zasady tworzenia dokumentacji projektowej” stanowiącym Załącznik nr 6 do Umowy.

3. Wymagania dla infrastruktury chmurowej

- 1) Wykonawca zapewni zasoby informatyczne usługi chmurowej, które Zamawiający będzie miał do dyspozycji w ramach etapów II-IV.
- 2) Zasoby informatyczne usługi chmurowej, o których mowa w ust. 3), 4) oraz 5), muszą być dostarczone w postaci umożliwiającej konfigurację i uruchomienie minimum 100 instancji maszyn wirtualnych pracujących jednocześnie.
- 3) W ramach Etapu II Umowy Wykonawca zapewni:
 - a) Liczba vCPU: 168 (procesory fizyczne o taktowaniu min. 2,2 Ghz)
 - b) Pamięć RAM: 296GB
 - c) Przechylenie dyskowa: 7TB, w tym (co najmniej 4 TB zbudowanej z dysków SSD)
 - d) Możliwość podpięcia do dodatkowego zasobu NFS, w ramach oferowanej przestrzeni dyskowej.
- 4) W ramach Etapu III Umowy Wykonawca zapewni:
 - a) Liczba vCPU: 256 (procesory fizyczne o taktowaniu min. 2,2 Ghz)
 - b) Pamięć RAM: 432GB
 - c) Przechylenie dyskowa: 20TB w tym (co najmniej 5 TB zbudowanej z dysków SSD)
 - d) Możliwość podpięcia do dodatkowego zasobu NFS, w ramach oferowanej przestrzeni dyskowej.
- 5) W ramach Etapu IV Umowy Wykonawca zapewni:
 - a) Liczba vCPU: 40 (procesory fizyczne o taktowaniu min. 2,2 Ghz)
 - b) Pamięć RAM: 64GB
 - c) Przechylenie dyskowa: 5TB
 - d) Możliwość podpięcia do dodatkowego zasobu NFS, w ramach oferowanej przestrzeni dyskowej.

- 6) Usługa chmurowa musi zapewniać dostęp do portalu administracyjnego dla Zamawiającego, umożliwiającego:
 - a) zarządzanie maszynami wirtualnymi, w tym ich tworzenie, usuwanie, migrację, zarządzanie zasobami poszczególnych maszyn, (vCPU, RAM, przestrzeń dyskowa),
 - b) dostęp do konfiguracji sieciowej i zarządzania pasmem,
 - c) monitorowanie użycia zasobów, o których mowa w ust. 1) i 2) oraz ruchu sieciowego.
 - d) tworzenie i zarządzanie użytkownikami w podziale na Administratorów uzyskujących dostęp do panelu zarządzania konfiguracją maszyn, sieci i monitorowania zasobów oraz Operatorów, uzyskujących dostęp do środowisk systemów operacyjnych maszyn wirtualnych.
- 7) Dostęp do panelu administracyjnego infrastruktury musi być możliwy z dowolnego miejsca poprzez przeglądarkę internetową (co najmniej połączenie szyfrowane SSL/TLS).
- 8) Usługa chmurowa musi zapewniać tworzenie maszyn wirtualnych w oparciu o własne lub predefiniowane szablony z systemami operacyjnymi Windows Server 2019, 2022 oraz Ubuntu.
- 9) Usługa chmurowa musi zapewniać możliwość zarządzania poprawkami systemu operacyjnego.
- 10) Usługa chmurowa musi umożliwiać migrację do chmury maszyn wirtualnych znajdujących się w infrastrukturze Zamawiającego (Hyper-V).
- 11) Usługa chmurowa musi zapewniać obsługę kontenerów.
- 12) Usługa chmurowa musi zapewniać możliwość konfiguracji sieci prywatnych, w których będą pracować maszyny wirtualne, w tym możliwość konfiguracji połączeń (portów TCP/UDP) pomiędzy poszczególnymi maszynami, oraz dopuszczenia ruchu z i do sieci Internet oraz sieci WAN, o której mowa w Rozdziale 4.
- 13) Usługa chmurowa musi umożliwiać tworzenie reguł NAT adresów maszyn wirtualnych z sieci VLAN na adresy publiczne.
- 14) Usługa chmurowa musi zapewniać przepływność wewnętrzną na poziomie min 10 Gb/s w odniesieniu do technologii IEEE 802.3.
- 15) Wykonawca będzie zapewniał dostęp do sieci Internet dla utworzonych przez Zamawiającego maszyn wirtualnych. Przepływność zewnętrzna w odniesieniu do parametrów MIR min symetrycznie 1 Gb/s.
- 16) Usługa chmurowa musi zapewniać nielimitowany transfer dla przesyłanych i pobieranych danych w ramach ruchu wewnętrznego i zewnętrznego.
- 17) Usługa chmurowa musi zapewniać szyfrowanie informacji przetwarzanych w chmurze, zarówno „at rest” jak i „in transit”.
- 18) W ramach ochrony kryptograficznej, usługa chmurowa musi zapewniać możliwość przechowywania kluczy w ramach infrastruktury własnej Zamawiającego.
- 19) Usługa chmurowa musi zapewniać możliwość szyfrowania informacji / danych podczas ich przechowywania i transmisji z zapewnieniem wyłącznej kontroli nad procesami generowania i zarządzania kluczami przez Zamawiającego.
- 20) Usługa chmurowa musi zapewniać konfigurację zapasowego środowiska przetwarzania danych (Disaster Recovery Center) oraz mechanizm automatycznego przełączania ruchu w przypadku awarii podstawowego centrum.
- 21) W ramach usługi chmurowej Wykonawca zapewni Zamawiającemu pulę min. 16 adresów publicznych IPv4.

- 22) Centra przetwarzania danych, w ramach których Wykonawca będzie świadczył usługę udostępniania zasobów chmurowych, muszą znajdować się na terytorium Rzeczypospolitej Polskiej lub na terytorium państwa Europejskiego Obszaru Gospodarczego.
- 23) Centra przetwarzania danych, o których mowa w pkt 18), muszą spełniać poniższe warunki:
- a) zasilanie z redundantnymi komponentami,
 - b) budynek objęty całodobowym systemem ochrony fizycznej (obecna na miejscu),
 - c) brak okien albo okna przeciwwłamaniowe (jeżeli parter) w pomieszczeniach serwerowni
 - d) drzwi antywłamaniowe z zamkiem antywłamaniowym,
 - e) dostęp do serwerowni zabezpieczony drzwiami antywłamaniowymi z zamkiem antywłamaniowym oraz ograniczony kartami magnetycznymi / kodem / kluczem deponowanym,
 - f) odnotowywanie każdego wejścia do pomieszczenia serwerowni (książka wejść / logi w systemie),
 - g) dostęp osób trzecich do serwerowni wyłącznie pod nadzorem,
 - h) brak elementów łatwopalnych na ścianach i suficie serwerowni,
 - i) klimatyzacja pomieszczeń serwerowni,
 - j) monitorowania środowiskowe serwerowni (min czujnik wilgoci i temperatury),
 - k) powiadamianie o anomaliach odczytu parametrów środowiskowych,
 - l) brak układów wodnokanalizacyjnych w pomieszczeniu serwerowni,
 - m) pomieszczenia serwerowni z podłogą techniczną, podniesioną ponad poziom kondygnacji,
 - n) system awaryjnego podtrzymania zasilania UPS pozwalający co najmniej na bezpieczne wyłączenie maszyn w przypadku awarii.
- 24) Usługa chmurowa musi umożliwiać podpięcie do wirtualnych maszyn zasobów NFS, w ramach oferowanej przestrzeni dyskowej.
- 25) Usługa chmurowa musi umożliwiać ręczne oraz automatyczne wykonywanie i przywracania kopii zapasowych przez Zamawiającego.
- 26) W ramach funkcjonalności wykonywania i odtwarzania kopii zapasowej, usługa chmurowa musi umożliwiać zarówno przywrócenie całej maszyny jak i pojedynczych plików z kopii zapasowej. Proces wykonywania kopii zapasowej maszyny nie zakłóci jej równoległego poprawnego funkcjonowania.
- 27) Wykonawca musi zapewnić dodatkowe zasoby (30TB dostępne od momentu odbioru Etapu II) na potrzeby wykonywania kopii zapasowych maszyn oraz zarządzanie kopiami zapasowymi (wykonywanie zgodnie z harmonogramem, przywracanie z kopii – obsługa kopii pełnych, przyrostowych i migawek).
- 28) Usługa chmurowa musi zapewniać zdalny oraz szyfrowany dostęp Operatorów, do środowisk systemów operacyjnych maszyn wirtualnych (RDP, SSH, konsola) utworzonych przez Zamawiającego.
- 29) Usługa chmurowa musi zapewniać rejestrację zdalnych sesji dostępu do systemów informatycznych. System musi aktywnie monitorować ruch w sieci i rejestrować wszelkie sesje dostępu SSH, RDP, HTTP, HTTPS.
- 30) Usługa chmurowa musi umożliwiać pobranie wszystkich danych przetwarzanych przez Zamawiającego, w szczególności maszyn wirtualnych oraz kopii zapasowych do własnej infrastruktury, w każdym momencie trwania Umowy.

- 31) Mechanizm pobierania danych Zamawiającego musi umożliwiać ich pełne bezpieczeństwo oraz integralności danych Zamawiającego.
- 32) Poziom transferu danych musi umożliwiać sprawne przeniesienie wszystkich danych Zamawiającego w czasie uzgodnionym przez Strony w Dokumentacji Powykonawczej.
- 33) Usługa chmurowa w obszarze realizacji zasad bezpieczeństwa musi spełniać wymagania techniczne i organizacyjne wynikające z regulacji określonych normą PN/ISO 27001 lub równoważną oraz z norm wynikających z przepisów prawa, w szczególności Rozporządzenia Rady Ministrów z dnia 12 marca 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a także aktualnie obowiązujących w tym zakresie regulacji prawnych, zmieniających lub zastępujących wskazane akty prawne. Usługa chmurowa musi zapewniać ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, w szczególności przez:
- a) monitorowanie wszelkich operacji wykonywanych w ramach chmury (w postaci logów),
 - b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
 - c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
 - d) dbałość o aktualizację oprogramowania i zabezpieczeń,
 - e) minimalizowanie ryzyka utraty informacji w wyniku awarii,
 - f) ochronę przed błędami, utratą, nieuprawnioną modyfikacją,
 - g) zgłaszanie Zamawiającemu incydentów mających wpływ na bezpieczeństwo przetwarzanych informacji,
 - h) niezwłoczne podejmowanie działań po dostrzeżeniu podatności mających wpływ na możliwość naruszenia bezpieczeństwa informacji.
- 34) Wykonawca zapewnia domyślną konfigurację usługi chmurowej w sposób uniemożliwiający dostawcy wgląd do przetwarzanych informacji.
- 35) Usługa chmurowa musi posiadać wdrożoną zasadę „minimum koniecznego” dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wymaganych przez Zamawiającego (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zgłoszeniem Zamawiającego a cały proces jest logowany.
- 36) Wymagane jest stosowanie następujących mechanizmów:
- a) ochrona i kontrola dostępu (zapora UTM - skrót od ang. Unified Threat Management) na styku z Internetem – odrzucanie niepożądanego ruchu sieciowego,
 - b) separacja ruchu kierowanego do urzędzeń na których przechowywane są dane klienta
 - c) system wykrywania i zapobiegania włamaniom (IDS/IPS – skrót od ang. Intrusion Detection System/ Intrusion Prevention System) oraz anty-DDOS.
- 37) Wykonawca musi zapewnić wsparcie techniczne dla świadczonej usługi chmurowej w systemie 24/7/365 oraz kanał do zgłaszania błędów i problemów dostępny w systemie 24/7/365.
- 38) Wykonawca zapewni dostępność usług chmurowych 24 godziny na dobę od poniedziałku do niedzieli, na poziomie 99% w ujęciu miesięcznym.

- 39) W ramach świadczonej usługi chmurowej, Wykonawca zapewni licencje na systemy operacyjne Windows Server 2019 oraz 2022, przeznaczone do zainstalowania i uruchomienia na maszynach wirtualnych o których mowa w pkt 1).
- 40) W ramach świadczonej usługi chmurowej, Wykonawca zapewni licencje na oprogramowanie antywirusowe, możliwe do zainstalowania i uruchomienia na maszynach wirtualnych o których mowa w ust. 1
- 41) W ramach świadczonej usługi chmurowej, Wykonawca zapewni licencje dostępowe do systemów operacyjnych, o których mowa w pkt 39) dla minimum 400 użytkowników.

4. Wymagania dla sieci WAN

- 1) W ramach Etapu V Umowy, Wykonawca zapewni i będzie utrzymywał sieć WAN komunikującą Partnerów Projektu oraz Zamawiającego z zasobami przetwarzanymi w ramach zaoferowanej usługi chmurowej (komunikacja „wiele do jednego” - topologia gwiazdy).
- 2) Ruch w sieci WAN musi być szyfrowany.
- 3) Sieć WAN musi uwzględniać logiczny podział na Partnerów Projektu e-kultura oraz e-biblioteki (zgodnie z Załącznikiem nr 5 do Umowy „Wykaz Punktów Odbioru Usługi”), oraz umożliwiać Zamawiającemu konfigurację ruchu sieciowego pomiędzy Partnerami i Zamawiającym (w Punktach Odbioru Usługi) a wybranymi zasobami chmury (np. (maszyny wirtualne, uruchomione na nich strony internetowe, API, usługi sieciowe, itp.)
- 4) Administrator musi mieć możliwość konfiguracji reguł dostępu pomiędzy środowiskiem chmurowym a poszczególnymi Punktami Odbioru Usługi (możliwość dopuszczenia ruchu na określonych portach).
- 5) Na czas trwania Umowy, Wykonawca zapewni niezbędne urządzenia potrzebne do poprawnego działania sieci WAN.
- 6) Wykonawca zapewni dostępność sieci WAN 24 godziny na dobę od poniedziałku do niedzieli, na poziomie 99% w ujęciu miesięcznym.
- 7) Wykonawca zapewni Zamawiającemu możliwość monitorowania stanu połączeń pomiędzy Punktami Odbioru Usługi a zasobami chmury w trybie 24 godzinny przez 7 dni w tygodniu.
- 8) Informacje historyczne oraz aktualne zbierane przez system monitorowania muszą być dostępne przez cały okres obowiązywania Umowy dla Zamawiającego.
- 9) Połączenie sieci WAN z zasobami Zamawiającego przetwarzanymi w chmurze musi zostać utrzymane również w wypadku przełączenia na zapasowe środowisko przetwarzania danych (Disaster Recovery Center).

5. Przeprowadzenie instruktaży dla Zamawiającego

- 1) Wykonawca zobowiązany jest do przeprowadzenia instruktażu dla osób wskazanych przez Zamawiającego w zakresie obsługi i zarządzania świadczonymi przez Wykonawcę usługami chmurowymi oraz siecią WAN.
- 2) Zakres instruktażu musi obejmować minimum zagadnienia związane z:
 - wykonywaniem i odtwarzaniem kopii zapasowych maszyn oraz konfiguracji uruchomionej w ramach usługi chmurowej,

- procedurą przejmowania działania przez zapasowe środowisko przetwarzania danych (Disaster Recovery Center),
 - uruchomianiem maszyn wirtualnych w oparciu o predefiniowany szablon z systemem operacyjnym oraz zaimportowany plik *.vhd,
 - zarządzaniem maszynami wirtualnymi
 - przydzielaniem Operatorom dostępu do wirtualnych maszyn,
 - zarządzaniem użytkownikami przez Administratorów,
 - tworzeniem, konfiguracją i zarządzaniem sieciami VLAN w chmurze,
 - udostępnianiem usług w sieci Internet,
 - konfigurowaniem komunikacji pomiędzy chmurą a Punktami Odbioru Usługi w ramach sieci WAN,
 - monitorowaniem użycia zasobów chmury oraz ruchu sieciowego,
 - monitorowaniem operacji wykonywanych w ramach chmury,
 - reagowaniem na najczęściej występujące incydenty bezpieczeństwa oraz awarie.
- 3) Na minimum 5 dni roboczych przed rozpoczęciem instruktaży Wykonawca zobowiązany jest do przygotowania i przekazania uczestnikom agendy instruktaży oraz materiałów szkoleniowych w języku polskim w postaci elektronicznej.
 - 4) Instruktaż musi obejmować minimum 1 dzień (6 godzin) dla grupy minimum 5 osób wskazanych przez Zamawiającego
 - 5) Instruktaże odbędą się w formie on-line. Na czas przeprowadzenia instruktaży, Wykonawca udostępni Zamawiającemu platformę telekonferencyjną, która będzie umożliwiała połączenie audio-video uczestników z prowadzącym oraz opcję udostępniania pulpitu zdalnego uczestnikom w celu wyświetlenia prezentacji.
 - 6) Wykonawca przedstawi i uzgodni z Zamawiającym termin przeprowadzenia instruktaży, na co najmniej 3 Dni Roboczych przed terminem ich rozpoczęcia.
 - 7) Osoby prowadzące instruktaże muszą posiadać wystarczającą wiedzę i doświadczenie w zakresie technologii, której dotyczy instruktaż.

6. Dokumentacja powykonawcza

- 1) Dokumentacja powykonawcza musi zostać przygotowana w języku polskim oraz zawierać co najmniej:
 - a) schemat i opis architektury sieci WAN, wyniki testów, sprawności usług;
 - b) wytyczne, wzorcowe konfiguracje, opisy zasad oraz politykę bezpieczeństwa usługi chmurowej, które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji.
 - c) dokumentację utrzymaniową Administratora, w tym m.in. :
 - sposób monitorowania infrastruktury,
 - sposób diagnozowania awarii,
 - opis najczęściej występujących problemów i awarii wraz z opisem procedur diagnostyczno-naprawczych,

- instrukcję reagowania na ataki sieciowe typu DDOS, ARP itp.,
 - instrukcję odzyskiwania konfiguracji w razie wystąpienia awarii.
- d) procedury administracyjne związane z bieżącą eksploatacją:
- instrukcję wykonywania i odtwarzania kopii zapasowych maszyn uruchomionych w ramach usługi chmurowej,
 - procedurę przejmowania działania przez zapasowe środowisko przetwarzania danych (Disaster Recovery Center),
 - instrukcję uruchomienia maszyn wirtualnych w oparciu o predefiniowany szablon z systemem operacyjnym oraz zaimportowany plik *.vhd,
 - instrukcję zarządzania maszynami wirtualnymi,
 - instrukcję przydzielania Operatorom dostępu do wirtualnych maszyn,
 - instrukcję zarządzania użytkownikami przez Administratorów,
 - instrukcję tworzenia, konfiguracji i zarządzania sieciami VLAN w chmurze,
 - instrukcję udostępniania usług w sieci Internet,
 - instrukcję konfiguracji komunikacji pomiędzy chmurą a Punktami Odbioru Usługi za pośrednictwem sieci WAN,
 - instrukcję monitorowania użycia zasobów chmury oraz ruchu sieciowego,
 - instrukcję monitorowania operacji wykonywanych w ramach chmury,
- e) procedury związane z usunięciem/migracją danych Zamawiającego:
- instrukcję/procedurę usuwania/migracji danych Zamawiającego przetwarzanych w zasobach usługi chmurowej, w tym wszystkich kopii zapasowych oraz danych znajdujących się w zapasowym środowisku przetwarzania danych
 - określenie czasu pobrania danych Zamawiającego do migracji,
 - szacunkowy harmonogram migracji danych Zamawiającego do innej usługi chmurowej lub infrastruktury własnej Zamawiającego,
 - określenie odpowiedzialności Stron,
 - niezbędne środki techniczne do realizacji migracji.
- 2) Dokumentacja, o której mowa w ust. 1, podlega odbiorowi przez Zamawiającego.
- 3) Dokumentacja o której mowa w ust. 1, musi zostać napisana zgodnie z dokumentem „Zasady tworzenia dokumentacji projektowej” stanowiącym Załącznik nr 6 do Umowy.

7. Warunki równoważności oprogramowania

- 1) Zamawiający dopuszcza zaoferowanie produktów równoważnych do dla Microsoft Windows Server 2019/2022.
- 2) Funkcjonalność oprogramowania równoważnego do Microsoft Windows Server 2019/2022:
 - a) System operacyjny musi być przeznaczony do instalacji w środowiskach serwerowych Data Center.
 - b) System operacyjny musi posiadać graficzny interfejs użytkownika.
 - c) System operacyjny musi być w pełni kompatybilny z usługą Active Directory.
 - d) System operacyjny musi umożliwiać uruchomienie roli kontrolera domeny Active Directory oraz tworzenie relacji zaufania między domenami.

- e) System operacyjny musi posiadać obsługę zdalnego pulpitu zgodnie z protokołem RDP.
- f) System operacyjny musi posiadać wbudowaną zaporę internetową dla ochrony połączeń internetowych.
- g) System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny.
- h) System operacyjny musi posiadać możliwość wdrożenia Active Directory Certificate Services.
- i) System operacyjny musi zapewniać automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- j) System operacyjny musi zapewniać szyfrowanie plików i folderów.
- k) System operacyjny musi posiadać możliwość narzucania wieloelementowej dynamicznej kontroli dostępu dla określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
- l) System musi umożliwiać instalację aplikacji w architekturze 32-bit oraz 64-bit.
- m) Licencje muszą uprawniać do instalacji systemu na maszynach wirtualnych funkcjonujących w ramach świadczonej przez Wykonawcę usługi chmurowej.
- n) Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych.
- o) Wszystkie wymienione powyżej parametry, role, funkcje systemu operacyjnego muszą być objęte dostarczoną licencją (licencjami) i nie wymagać ponoszenia przez Zamawiającego dodatkowych kosztów.