**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Rozbudowa infrastruktury fizycznej oraz środowiska wirtualnego**

**na potrzeby Centrum Projektów Polska Cyfrowa**

**SPIS TREŚCI**

[1 SŁOWNIKI I SKRÓTY 3](#_Toc514405906)

[2 CEL ZAMÓWIENIA 6](#_Toc514405907)

[2.1 Wprowadzenie: 6](#_Toc514405908)

[3 PRZEDMIOT ZAMÓWIENIA 7](#_Toc514405909)

[4 WYMAGANIA Z ZAKRESIE URZĄDZEŃ i OPROGRAMOWANIA 11](#_Toc514405910)

[4.1 Serwery 11](#_Toc514405911)

[4.2 Oprogramowanie do wirtualizacji (3 hosty fizyczne) 15](#_Toc514405912)

[4.3 Macierz 1 szt. 17](#_Toc514405913)

[4.4 Urządzenia sieciowe 21](#_Toc514405914)

[4.4.1 Urządzenie sieci LAN, przełącznik – 2 szt. 21](#_Toc514405915)

[5 SYSTEM KOPII BEZPIECZEŃSTWA 25](#_Toc514405916)

[5.1 Wymagania dotyczące Systemu Kopii Bezpieczeństwa (SKB) 26](#_Toc514405917)

[6 ŚWIADCZENIE USŁUGI SERWISU I GWARANCJI 31](#_Toc514405918)

[7 WYMAGANIA DOTYCZĄCE USŁUGI INSTALACJI URZĄDZEŃ. 34](#_Toc514405919)

[8 MINIMALNE WYMAGANIA W ZAKRESIE USŁUGI WDROŻENIA. 34](#_Toc514405920)

[9 WYMAGANIA W ZAKRESIE WARSZTATÓW. 35](#_Toc514405921)

[10 WYMAGANIA W ZAKRESIE DOKUMENTACJI 37](#_Toc514405922)

[11 WYMAGANIA W ZAKRESIE OZNAKOWANIA URZĄDZEŃ i DOKUMENTACJI 41](#_Toc514405923)

[12 WYMAGANIA W ZAKRESIE DOSTĘPNOŚCI 42](#_Toc514405924)

[13 WYMAGANIA W ZAKRESIE ZGODNOŚCI Z PRZEPISAMI PRAWA 42](#_Toc514405925)

# SŁOWNIKI I SKRÓTY

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

| **Skrót/pojęcie** | **Definicja** |
| --- | --- |
| **Awaria** | Oznacza sytuację uniemożliwiająca użytkownikom prawidłowe lub pełne korzystanie z Urządzeń, Oprogramowania, wadę lub usterkę Urządzenia, Oprogramowania. |
| **Błąd** | Oznacza Błąd Krytyczny i/lub Błąd Niekrytyczny i/lub Błąd Zwykły; |
| **Błąd Krytyczny** | Oznacza brak działania środowiska produkcyjnego Systemu, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Błędy Krytyczne mają jedną lub więcej z poniższych cech:   1. dane biznesowe zostały uszkodzone; 2. Funkcjonalność Krytyczna udokumentowana w Projekcie Technicznym Uzupełnień nie działa; 3. System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji; 4. wszelkie błędy związane z bezpieczeństwem przechowywania  i przetwarzania danych, które mogą wpłynąć na:    1. uwierzytelnianie,    2. niezaprzeczalność,    3. poufność,    4. integralność,    5. dostępność,    6. rozliczalność, 5. wszelkie błędy związane z bezpieczeństwem dostępu  do Systemu (w tym nieautoryzowanym dostępem do danych); |
| **Błąd Niekrytyczny** | Utrudnia działanie Systemu w środowisku produkcyjnym w zakresie Funkcjonalności Krytycznej i uniemożliwia działanie Systemu  w zakresie pozostałych funkcjonalności. W tym kontekście „utrudnia” oznacza istnienie sposobu jego obejścia, stosując przygotowane przez Wykonawcę procedury tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji, (co może mieć wpływ na wygodę w użytkowaniu Systemu lub wymagać procedur ręcznych). „Uniemożliwia” oznacza brak możliwości jego obejścia; |
| **Błąd Zwykły** | Wszelki błąd niebędący Błędem Krytycznym lub Błędem Niekrytycznym; |
| **Dane** | Należy przez to rozumieć dane dotyczące abonenta, o których mowa  w art. 161 ust. 2 pkt. 4–6 oraz art. 169 ust. 1 ustawy z dnia 16 lipca  2004 r. — Prawo telekomunikacyjne; |
| **Dni Robocze** | Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 16.00; |
| **Dokumentacja** | Wytworzone przez Wykonawcę w ramach realizacji Umowy i podlegające zatwierdzeniu przez Zamawiającego materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności Projekt Infrastruktury Fizycznej Systemu, Projekt Techniczny, Wykaz Ilościowo-Cenowy, Plan Wdrożenia, Plan Testów Akceptacyjnych (PTA), Plan Zarządzania Projektem (PZP), Dokumentacja Powykonawcza, Dokumentacja Eksploatacyjna, Dokumentacja Powdrożeniowa Systemu, Plan Rozwoju Systemu, Opis Realizacji Warsztatów, materiały warsztatowe, dokumentacja powstała w wyniku realizacji wymagań odbioru produktów, dokumentacja powstała w wyniku realizacji wymagań zarządzania projektem, dokumenty robocze wytworzone przez Wykonawcę w ramach realizacji Umowy; za Dokumentację uznaje się także wytworzenie i aktualizację Dokumentacji w ramach modyfikacji i Nadzoru Autorskiego oraz w okresie gwarancji i świadczenia usług serwisu gwarancyjnego; |
| **Funkcjonalności Krytyczne** | Cechy funkcjonalne środowiska produkcyjnego:  Wirtualizacja serwerów, wykonywanie kopii bezpieczeństwa, przechowywanie kopii bezpieczeństwa, przywracanie systemów z kopii bezpieczeństwa w środowiskach produkcyjnych i zapasowych, replikacja w środowisku zapasowym poprzez sieć Internet w ramach VPN, transmisja danych sieciowych pomiędzy serwerami, oraz pomiędzy serwerami i macierzą dyskową, transmisja danych pomiędzy środowiskiem produkcyjnym a siecią Internet.  W ramach środowiska produkcyjnego i wymienionych cech funkcjonalnych będą uruchomione funkcjonalności krytyczne polegające na: świadczenie usług serwerów sieci web, poczty elektronicznej, kontroler domeny, usługa nazw, systemu obiegu dokumentacji elektronicznej, systemy finansowo-księgowegowe, serwer plików, serwery baz danych, serwery wysokiej dostępności. |
| **Incydent serwisowy** | Oznacza zgłoszenie do Wykonawcy przez Zamawiającego lub osoby wskazane przez Zamawiającego, w trybie **24 godziny na dobę 7 dni** **w tygodniu**, nieprawidłowości w działaniu Systemu. Wykonawca zobowiązany jest do rejestracji zgłoszenia oraz usuwania Błędów i usterek lub dostarczenia procedur obejścia, powodujących przywrócenie działania Systemu i rozwiązania zgłoszenia; |
| **Informacje** | Należy przez to rozumieć informacje, o których mowa w art. 78  ust. 3 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne; |
| **Lokalizacja Podstawowa** | Oznacza pomieszczenie w siedzibie Zamawiającego, do którego Wykonawca dostarczy Urządzenia i Oprogramowanie wraz z odnoszącą się dokumentacją techniczną producenta będące przedmiotem niniejszego zamówienia; |
| **Lokalizacja Zapasowa** | Oznacza pomieszczenie w serwerowni wynajmowanej przez Zamawiającego, do którego Wykonawca przeniesie skonfigurowane Urządzenia i Oprogramowanie wchodzące w skład Środowiska Zapasowego; |
| **Środowisko podstawowe** | Oznacza Urządzenia i Oprogramowanie w Lokalizacji Podstawowej w ramach którego będą funkcjonować usługi produkcyjne. |
| **Środowisko zapasowe** | Oznacza Urządzenia i Oprogramowanie w Lokalizacji Zapasowej w ramach którego będzie wykonywana replikacja z Lokalizacji Podstawowej, testy odtworzeniowe i awaryjne uruchomienie usług. |
| **Nadzór Autorski** | Czynności Wykonawcy wykonywane w ramach Zleceń polegające  na doradztwie i konsultacjach technicznych, Modyfikacjach oraz pracach związanych z rozbudową, zmianami, usprawnieniami oraz zmianą konfiguracyjną Systemu, oraz dokonywanie zmian Dokumentacji, zgodnie z oczekiwaniami Zamawiającego lub Użytkowników wraz z przeniesieniem w ramach wynagrodzenia za poszczególne Zlecenia majątkowych praw autorskich oraz praw zależnych do zmienionej Dokumentacji; |
| **Oprogramowanie** | Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci. Zamawiający dopuszcza zastosowanie Oprogramowania w poniższych obszarach:   1. system operacyjny, 2. oprogramowanie bazodanowe, 3. oprogramowanie do tworzenia raportów, 4. oprogramowanie do archiwizacji i tworzenia kopii bezpieczeństwa, 5. oprogramowanie do wirtualizacji, 6. oprogramowanie narzędziowe do monitorowania i diagnozy Systemu,   Każde Oprogramowanie musi uzyskać akceptację Zamawiającego najpóźniej na etapie Projektu Technicznego; |
| **Plan Testów Akceptacyjnych /PTA** | Dokument opracowany przez Wykonawcę podlegający akceptacji Zamawiającego; |
| **Projekt Techniczny** | Projekt Techniczny Uzupełnień, element Dokumentacji opisujący sposób wykonania, wdrożenia i właściwości Uzupełnień do poziomu Systemu. Szczegółowe wymagania dla Projektu Technicznego zostały określone w wymaganiu DOK.1.1; |
| **Plan Zarządzania**  **Projektem / PZP** | Element Dokumentacji definiujący organizację procesy, narzędzia i  techniki dobrane w celu skutecznej i efektywnej realizacji przedmiotu  Umowy, zawierający, co najmniej: szczegółowy opis zadań  realizowanych w ramach Etapów, harmonogram, plan komunikacji,  szczegółowe procedury rejestracji zgłoszenia i obsługi Błędów realizowanych w ramach serwisu gwarancyjnego. |
| **SLA** | Service Level Agreement, poziom dostępności usług |
| **System** | Infrastruktura sprzętowo - programowa, powstała w wyniku realizacji Umowy. System składa się z:  - Urządzeń,  - Oprogramowania. |
| **System Kopii Bezpieczeństwa / SKB** | Urządzenia i Oprogramowanie Standardowe służące kopiowaniu na nośniki zewnętrzne danych (w szczególności: pliki, bazy danych, rejestry, konfiguracje) gromadzonych na infrastrukturze serwerowej realizowany w ramach niniejszego przedmiotu zamówienia. |
| **Replikacja** | Funkcjonalność polegająca na automatycznym, okresowym asynchronicznym przenoszeniu kopii obrazów maszyn wirtualnych z Środowiska Produkcyjnego do Zapasowego. |
| **Umowa** | Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia; |
| **Urządzenia** | Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i odnoszącą się do nich dokumentacją techniczną producenta, w tym również okablowanie strukturalne, będące przedmiotem niniejszego zamówienia; |
| **Urządzenia Zamawiającego** | Sprzęt teleinformatyczny z oprogramowaniem wraz z niezbędnym wyposażeniem, funkcjonujący aktualnie u Zamawiającego jako Środowisko Podstawowe, które zostaną wykorzystane do budowy Środowiska Zapasowego; |
| **Usługa Serwisu** | Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Systemu oraz jego poszczególnych komponentów, w szczególności usuwanie Błędów; |
| **Wykonawca/Dostawca** | Podmiot realizujący zamówienie; |
| **Zamawiający** | Centrum Projektów Polska Cyfrowa; |
| **Zlecenie** | Oznacza zamówienie złożone przez Zmawiającego będące podstawą realizacji przez Wykonawcę Nadzoru Autorskiego, w tym modyfikacji oraz Warsztatów; |

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

# CEL ZAMÓWIENIA

Zamówienie polega na przebudowie infrastruktury serwerowo-macierzowej oraz instalacji środowiska wirtualnego na potrzeby funkcjonowania środowiska produkcyjnego Centrum Projektów Polska Cyfrowa i uruchamiania nowych usług. W ramach Zamówienia na Przebudowę Infrastruktury, Wykonawca zaprojektuje, dostarczy nowe Urządzenia, Oprogramowanie, Dokumentację oraz wykorzysta obecne funkcjonujące Urządzenia i Oprogramowanie wyodrębnienie z istniejących zasobów Zamawiającego do stworzenia Środowiska Podstawowego i Środowiska Zapasowego, która będzie docelowo funkcjonować w Lokalizacji Podstawowej i Zapasowej. Wykonawca przeprowadzi niezbędne Warsztaty dla Administratorów.

Postępowanie obejmuje również dostawę i konfigurację Systemu Kopii Bezpieczeństwa z replikacją do Środowiska Zapasowego, wraz z usługą migracji wszystkich obecnych zasobów (maszny wirtualne wraz z Danymi) określonych w Projekcie Technicznym z uwzględnieniem okoliczności dodatkowej konfiguracji lub/i rozszerzenia posiadanych licencji przez Zamawiającego w celu poprawnego funkcjonowania zaprojektowanego rozwiązania.

## Wprowadzenie:

Obecne środowisko zlokalizowane jest w serwerowni przy ulicy Spokojnej 13A w Warszawie, składa się z 4 serwerów fizycznych w tym 3 dedykowane do pracy na potrzeby środowiska wirtualnego (około 40 maszyn wirtualnych) Vmware 6, macierzy dyskowej wraz z półkami dyskowymi, dwóch przełączników, dwóch routerów i UPS.

Zamawiający zakłada, że dostarczone rozwiązanie będzie wykorzystywało elementy obecnej infrastruktury. Wykonawca zamontuje, skonfiguruje i uruchomi dostarczone urządzenia w szafie Rack 19” Zamawiającego. Wykonawca powinien podłączyć dostarczone urządzenia do urządzenia UPS Zamawiającego. Wszelkie szczegóły zostaną sprecyzowane w Projekcie Technicznym.

# PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest:

* dostawa nowych lub aktualizacja obecnych licencji przez Wykonawcę Oprogramowania do wirtualizacji, zarządzania maszynami wirtualnymi, zarządzania Urządzeniami oraz konfiguracja zgodnie z założeniami Zamawiającego;
* dostawa oprogramowania Systemu Kopii Bezpieczeństwa (SKB) oraz konfiguracja według założeń Zamawiającego;
* dostawa przez Wykonawcę serwerów, macierzy dyskowych i urządzeń sieciowych - przełączników sieciowych, niezbędnego okablowania wraz z oprogramowaniem wbudowanym niezbędnym do prawidłowego działania sprzętu, konfiguracja według założeń Zamawiającego;
* migracja obecnych serwerów wirtualnych, z uwzględnieniem architektury sieci Zamawiającego, konfiguracja nowego Środowiska Podstawowego i Środowiska Zapasowego według Projektu Technicznego;
* przeprowadzenie warsztatów z zakresu obejmującego rozwiązania zastosowane przez Wykonawcę;
* udzielenia gwarancji i zapewnienie Serwisu Gwarancyjnego oraz Nadzoru Autorskiego,
* rozszerzenie gwarancji i zapewnienie serwisu gwarancyjnego na elementy obecnej infrastruktury według założeń Zamawiającego;
* dostarczenia Dokumentacji według założeń Zamawiającego;

Przedmiot zamówienia obejmuje:

|  |  |  |  |
| --- | --- | --- | --- |
| **Etapy** | **Przedmiot zamówienia** | **Maksymalny czas wyznaczony do realizacji Etapu** | **Minimalny czas wymagany do realizacji poszczególnych zadań w ramach Etapu** |
| **Etap 1** | 1. Opracowanie i dostarczenie Zamawiającemu Dokumentacji Etapu 1, w szczególności: 2. Projektu Infrastruktury Fizycznej Systemu – uwzględniającej Środowisko Podstawowe i Środowisko Zapasowe; 3. Projektu Technicznego; 4. Planu Zarządzania Projektem; 5. Przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu 1 wraz z prawem zezwalania na wykonywanie praw zależnych, na zasadach określonych w istotnych postanowieniach umowy; 6. Dostawa do Lokalizacji Podstawowej Urządzeń i Oprogramowania; udzielenie licencji na dostarczone w ramach tego etapu Umowy Oprogramowanie oraz dostarczanie aktualizacji Oprogramowania w okresie gwarancji wraz z udzieleniem licencji na dostarczone aktualizacje; | **15 dni** **od dnia podpisania Umowy** | 3 Dni Robocze na czynności odbiorcze Zamawiającego |
| **Etap 2** | 1. Opracowanie i dostarczenie Zamawiającemu Dokumentacji Etapu 2, w szczególności:    1. Planu Testów Akceptacyjnych,    2. Planu Wdrożenia,    3. Opisu Realizacji Warsztatów. 2. Instalacja, konfiguracja, uruchomienie zgodnie z zaakceptowanym Projektem Technicznym oraz Planem Wdrożenia odebranych przez Zamawiającego, Urządzeń i Oprogramowania; 3. Przeprowadzenie Testów Akceptacyjnych Systemu, zgodnie z zatwierdzonym przez Zamawiającego Planem Testów Akceptacyjnych; 4. Przeprowadzenie wdrożenia produkcyjnego wraz z migracją danych Systemu zgodnie z Projektem Technicznym oraz Planem Wdrożenia; 5. Przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu 2 wraz z prawem zezwalania na wykonywanie praw zależnych, na zasadach określonych w istotnych postanowieniach umowy; | **35 dni od dnia** **podpisania Umowy**, | 5 Dni Roboczych na czynności odbiorcze po stronie Zamawiającego dot. Etapu 2. |
| **Etap 3** | 1. Opracowanie i dostarczenie Zamawiającemu Dokumentacji w szczególności:   a) Dokumentacji Powykonawczej,  b) Dokumentacji Eksploatacyjnej,  c) Dokumentacji Powdrożeniowej Systemu  d) Wykaz Ilościowo-Cenowy;   1. Przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu 3 wraz z prawem zezwalania na wykonywanie praw zależnych, na zasadach określonych w istotnych postanowieniach umowy; | **50 od dnia** **podpisania Umowy**, | 5 Dni Roboczych na czynności odbiorcze po stronie Zamawiającego dot. odbioru Etapu 3. |
| **Nadzór Autorski** | 1. Świadczenie Nadzoru Autorskiego w wysokości 150 roboczogodzin, gdzie roboczogodzina oznacza 60 minut, w okresie 60 miesięcy od podpisania protokołu odbioru Etapu 3. | **W okresie 60 miesięcy od podpisania Protokołu Odbioru Etapu 3 lub do wcześniejszego wyczerpania przyjętego limitu roboczogodzin** | 3 Dni Robocze na czynności odbiorcze po stronie Zamawiającego dotyczące odbioru Zlecenia nadzoru autorskiego. |
| **Warsztaty** | 1. Przeprowadzanie przez Wykonawcę warsztatów, w zakresie administrowania Systemem dla 3 osób, realizowanych na podstawie Zleceń; | **od dnia podpisania protokołu odbioru Etapu 2 do upływu 6 miesięcy od podpisania protokołu odbioru Etapu** | 3 Dni Robocze na czynności odbiorcze po stronie Zamawiającego dotyczące każdorazowego odbioru Zlecenia przeprowadzenia warsztatów. |
| **Gwarancja** | 1. Udzielenie gwarancji i świadczenie usługi serwisu gwarancyjnego dla Systemu, w tym Urządzeń i Oprogramowania w okresie 36 miesięcy od podpisania protokołu odbioru Etapu 2, oraz na prace wykonane w ramach Nadzoru Autorskiego, w tym Modyfikacje, od dnia podpisania danego Protokołu Odbioru Zlecenia na podstawie, którego prace te są odbierane do upływu 36 miesięcy od dnia podpisania Protokołu Odbioru Etapu 2; | **Gwarancja na Urządzenia i Oprogramowanie Standardowe dostarczone w ramach Etapu 1 biegnie od dnia podpisania Protokołu Odbioru Urządzeń, w pozostałym zakresie od dnia podpisania Protokołu Odbioru Etapu 2, w okresie 36 miesięcy od podpisania protokołu odbioru Etapu 2, oraz na prace wykonane w ramach Nadzoru Autorskiego, w tym Modyfikacje, od dnia podpisania danego Protokołu Odbioru Zlecenia na podstawie, którego prace te są odbierane do upływu 36 miesięcy od dnia podpisania Protokołu Odbioru Etapu 2** |  |

# WYMAGANIA Z ZAKRESIE URZĄDZEŃ i OPROGRAMOWANIA

W ramach Umowy Urządzenia dostarczone przez Wykonawców winny zostać zamontowane oraz zainstalowane i uruchomione w Lokalizacji wskazanej przez Zamawiającego. Lokalizacja oraz warunki techniczne zostaną przedstawione na etapie Projektu Technicznego.

Jeżeli nie nadmieniono to należy uznać, że wszystkie urządzenia sieciowe, serwery, macierze powinny być dostarczone wraz z przypisanymi do Urządzeń licencjami.

Dodatkowo jeśli nie wskazano to należy uznać, że wszystkie Urządzenia powinny być dostarczone wraz z niezbędnym do instalacji okablowaniem.

O ile inaczej nie zaznaczono, wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.

Zaoferowane przez Wykonawcę urządzenia Sytemu muszą być fabrycznie nowe, nieużywane, wyprodukowane nie wcześniej niż w okresie ostatnich 12 miesięcy.

## Serwery

**Serwer produkcyjny - 3 szt:**

Serwery są przewidziane jako serwery działające na rzecz środowiska wirtualnego pracującego jako uruchomiane w klastrze HA platformy witalizacyjnej.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
|  | Procesor: Zainstalowane dwa procesory min. ośmio-rdzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem. Procesor taktowany o częstotliwości min. 1,8Ghz oraz posiadający min. 11MB pamięci podręcznej. |
|  | RAM: 384GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci z których maksymalnie 12 powinno być zajętych. Instalacja pamięci powinna umożliwiać w przyszłości rozszerzenie pojemności. Płyta główna powinna obsługiwać co najmniej 512GB pamięci RAM. |
|  | Zabezpieczenia pamięci RAM: Memory Rank Sparing, Memory Mirror, Lockstep |
|  | Gniazda PCI: min. 2 sloty PCIe x16. |
|  | Interfejsy sieciowe/FC: Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T. Zainstalowane dwie karty dwuportowe 10 GbE lub wbudowane Interfejsy w standardzie Base-T. |
|  | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
|  | Dedykowany Chipset przez producenta procesora do pracy w serwerach dwuprocesorowych. |
|  | Kontroler RAID: Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. Wsparcie dla dysków samoszyfujących. |
|  | Dyski twarde: Zainstalowane 2x120GB SSD SATA 6Gb/s.  Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia modułu w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.  Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID 1. |
|  | Zamawiający nie wymaga napędu optycznego. |
|  | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack.  Przedni panel zamykany na klucz. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
|  | Serwer musi posiadać redundantne wentylatory. |
|  | Serwer musi mieć redundantne zasilanie, Hot-Plug maksymalnie 550W. |
|  | Serwer musi posiadać zintegrowana kartę graficzną umożliwiającą wyświetlenie rozdzielczości min. 1920x1200. |
|  | Urządzenie musi mieć min. 3 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
|  | Zamawiający nie wymaga dostarczenia systemu operacyjnego do serwera. |
|  | Serwer musi być dostarczony z zestawem szybkiego montażu, czyli z wszelkimi elementami montażowymi szafy do szafy 19” np. śruby, nakrętki, uchwyty, maskownice, szyny, prowadnice na kable i inne elementy, wymagane do późniejszej prawidłowej i bezpiecznej instalacji i eksploatacji urządzeń w szafach. |
|  | Zamawiający wymaga aby niezależne od zainstalowanego na serwerze systemu operacyjnego, funkcjonowała karta zarządzania posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiający:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) * szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI 2.0, VLAN tagging, Telnet, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez dwóch administratorów jednocześnie * wsparcie dla dynamic DNS * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232. * Producent systemu musi posiadać dedykowane rozwiązanie, które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe. * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. * możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów. * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi. * możliwość zablokowania konfiguracji oraz odnowienia oprogramowania  karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty.   Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów – WMI, SNMP, IPMI, Linux SSH * Możliwość oskryptowywania procesu wykrywania urządzeń * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS * Grupowanie urządzeń w oparciu o kryteria użytkownika * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.   Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) |
|  | Serwer musi posiadać Moduł TPM 2.0 oraz wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
|  | Z serwerem należy dostarczyć następujące certyfikaty:   1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. 2. Serwer musi posiadać deklarację CE. 3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2, Windows Server 2016. |
|  | Warunki gwarancji. Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzone dyski pozostają własnością Zamawiającego. |
|  | Dokumentacja użytkownika. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |
|  | Zamawiający oczekuje, że będzie możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego. |

## Oprogramowanie do wirtualizacji (3 hosty fizyczne)

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
|  | Dostarczane oprogramowanie do wirtualizacji musi poprawnie współpracować z posiadanym przez Zamawiającego oprogramowaniem VMWare 6.0, szczególnie w zakresie kompatybilności formatów danych i protokołów. |
|  | Dostarczane oprogramowanie do wirtualizacji musi pozwalać na zarządzanie pojedynczym serwerem fizycznym (hostem) przynajmniej za pomocą:   * klienta graficznego (GUI) bez konieczności zakupu dodatkowych licencji możliwość instalacji na Windows Server 2008R2 i nowszym, Windows 7/8 64 bit i nowszym), * linii komend (CLI) dostępnej poprzez SSH. |
|  | Dostarczane oprogramowanie do wirtualizacji musi umożliwiać tworzenie maszyn wirtualnych oraz ich konfigurację. |
|  | Obsługa minimum 4 wirtualnych rdzeni CPU dla jednej maszyny wirtualnej opartej na Microsoft Windows 7/8.1/2008/2012 lub nowszej. |
|  | Dostarczane oprogramowanie do wirtualizacji musi umożliwiać instalację na maszynach z przynajmniej 2 CPU fizycznym złączem oraz przynajmniej 128GB RAM. |
|  | Dostarczane oprogramowanie do wirtualizacji musi pozwalać na obsługę wielu instancji systemów operacyjnych na jednym serwerze fizycznym. |
|  | Dostarczane oprogramowanie do wirtualizacji musi mieć możliwość zarządzania przydziałem zasobów maszyny wirtualnej (przydzielanie pamięci RAM, procesorów, dysków twardego). |
|  | Dostarczane oprogramowanie do wirtualizacji musi pozwalać na instalację maszyn wirtualnych przynajmniej z następującymi systemami operacyjnymi:   * Debian 64 bit, * Ubuntu 64 bit, * Windows 7, 8, 10, * Windows Server 2008R2, 2012R2, 2016 i nowszych. |
|  | Dostarczane oprogramowanie do wirtualizacji musi umożliwiać automatyczne uruchomienie maszyny wirtualnej po awarii i restarcie serwera fizycznego (hosta) na którym działało. |
|  | Dostarczane oprogramowanie do wirtualizacji musi wspierać konfigurację wysokiej dostępności (HA). |
|  | Dostarczane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek. |
|  | Dostarczane oprogramowanie do wirtualizacji musi posiadać możliwość konfiguracji wielu wirtualnych przełączników, z których każdy:   * umożliwia tworzenie sieci wirtualnej w obszarze hosta, * pozwala połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej, * obsługuje wirtualne sieci lokalne zgodnie ze standardem IEEE 802.1q (VLAN), * posiada możliwość przyłączania do niego przynajmniej dwóch fizycznych kart sieciowych hosta aby zapewnić bezpieczeństwo połączenia sieciowego w razie awarii karty sieciowej. |
|  | Możliwość instalacji oprogramowania do wirtualizacji na 3 urządzeniach typu rack z 2 fizycznymi procesorami każdy niezależnie od ilości umieszczonych w nich rdzeni wykonawczych. W przypadku wystąpienia sytuacji w której producent oprogramowania wbudowanego, oprogramowania do wirtualizacji lub oprogramowania do zarządzania maszynami wirtualnymi zmieni sposób licencjonowania oprogramowania, wówczas Wykonawca musi dostarczyć oprogramowanie i licencje adekwatne do zamówienia. |
|  | W ramach dostarczonego oprogramowania do wirtualizacji, Wykonawca musi zapewnić minimum 60 miesięcy asysty technicznej zawierającej również wsparcie w przypadku wystąpienia błędów oprogramowania. |
|  | Dostarczane oprogramowanie wspierające zarządzanie maszynami wirtualnymi musi poprawnie współpracować z dostarczonym przez Wykonawcę oprogramowaniem do wirtualizacji. |
|  | Dostarczane oprogramowanie wspierające musi umożliwiać centralne zarządzanie środowiskiem do wirtualizacji (m. in. hostami, maszynami wirtualnymi, współdzielonymi magazynami danych) Zamawiającego wytworzonymi przy pomocy dostarczonego oprogramowania do wirtualizacji , za pomocą:   * klienta graficznego bez konieczności zakupu dodatkowej licencji (możliwość instalacji na Windows Server 2008R2 i nowszym, Windows 7/8 64 bit), * webowe GUI do zarządzania środowiskiem wirtualnym (za pomocą przynajmniej przeglądarki Firefox w wersji 35 i nowszej, Internet Explorer 10 i nowszej, Chrome 35 i nowszej). |
|  | Dostarczane oprogramowanie wspierające musi pozwalać na centralne zarządzanie infrastrukturą złożoną z przynajmniej 3 dwuprocesorowych hostów. |
|  | Dostarczane oprogramowanie wspierające musi umożliwiać zdalne zarządzanie maszynami wirtualnymi i monitorowanie stanu ich pracy (m.in. utylizacja procesora, utylizacja pamięci utylizacja dysku, utylizacja interfejsów). |
|  | Dostarczane oprogramowanie wspierające musi umożliwiać analizę i wizualizację stanu infrastruktury. |
|  | Dostarczane oprogramowanie wspierające musi umożliwiać konfigurację parametrów wysokiej dostępności (HA) serwera fizycznego (hosta), aby w przypadku awarii lub niedostępności hosta wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach infrastruktury z zainstalowanym oprogramowaniem do wirtualizacji. |
|  | Dostarczane oprogramowanie wspierające musi umożliwiać wykonywania kopii migawkowych maszyn wirtualnych (tzw. snapshot). |

## Macierz 1 szt.

Przez **macierz dyskową** Zamawiający rozumie zestaw dysków twardych kontrolowanych przez kontrolery macierzowe i udostępniający wspólną przestrzeń dyskową bez zastosowania zewnętrznych wirtualizatorów. Za pojedynczą macierz nie można uznać rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
|  | Macierz dyskowa musi być dostarczona z minimum 17 dyskami o pojemności minimum 1,8TB/10k RPM. |
|  | Macierz dyskowa musi mieć możliwość podłączenia dodatkowych dysków twardych o parametrach:   * dyski SSD o pojemności minimum 1,6TB, 3,2TB oraz * dyski SATA lub NL-SAS o pojemności minimum 6TB oraz * dyski SAS o pojemności minimum 1.2TB |
|  | Macierz musi mieć możliwość utworzenia grupy RAID w której dwa dyski, które będą przechowywać dane parzystości. |
|  | Awaria dwóch dowolnych dysków w obrębie takiej pojedynczej grupy RAID nie może spowodować utraty danych. |
|  | Kontrolery macierzy dyskowej muszą obsługiwać minimum 148 dysków |
|  | Macierz musi mieć możliwość rozbudowy on-line (przy ciągłym dostępie hostów do danych składowanych na macierzy) do 500 dysków. |
|  | Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (High Availability Cluster). Każdy kontroler musi posiadać identyczną konfigurację, tzn. liczbę i parametry CPU, parametry i pojemność pamięci cache, parametry i liczbę portów we/wy.Te same kontrolery muszą udostępniać dane poprzez iSCSI, FCP, CIFS oraz NFS. |
|  | Obszar pamięci cache przeznaczony do zapisów danych, musi posiadać lustrzaną kopię (ang. mirror). |
|  | Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze. |
|  | Macierz musi mieć minimum 256GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. |
|  | Każdy kontroler musi mieć możliwość obsługi dodatkowej pamięci cache w postaci dysków, które mają być wykorzystywane jako oddzielny obszar pamięci dla bloków danych odczytywanych i nadpisywanych |
|  | System operacyjny kontrolerów musi natywnie obsługiwać automatyczny tiering bloków danych pomiędzy dyskami SSD, SAS, NL\_SAS. |
|  | Macierz dyskowa musi obsługiwać sumarycznie minimum 768GB pamięci SSD cache. |
|  | Każdy kontroler musi pracować pod kontrolą jednego systemu operacyjnego stworzonego przez producenta urządzenia. Nie dopuszcza się zastosowania systemu, w którym udostępnianiem danych zarządzają różne systemy operacyjne w jednym zintegrowanym urządzeniu. |
|  | Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych. |
|  | Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 128TB i plikowych o rozmiarze minimum 64TB. |
|  | Każdy kontroler musi być wyposażony w następujące działające porty/interfejsy:   * 2 porty 10GE Base-T oraz 2 porty 10Gbps SFP+ do podłączania hostów i replikacji – porty muszą być obsadzone odpowiednimi wkładkami SFP+ SR * 1 port 1GbE Base-T do zdalnego zarządzania kontrolerem * 2 porty SAS minimum 6Gbs do podłączania półek dyskowych * 1 port konsolowy |
|  | System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie Copy-On-Write. |
|  | Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika. |
|  | System operacyjny macierzy dyskowej musi umożliwiać i wykonywanie kopii migawkowych wolumenów plikowych, w trybie on-line, bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 255 na wolumen. |
|  | Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny. |
|  | Musi być możliwe zaprezentowanie kopii migawkowej w trybie do odczytu i zapisu. |
|  | Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji w minimum wersjach:  Exchange 2016 i nowsze, SQL Server 2008 i 2012 i nowsze, VMware dla blokowych i plikowych datastore.  Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych.  Oprogramowanie to musi rozpoznać na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. |
|  | 1.System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i iSCSI - jeśli do uruchomienia potrzebna jest licencja to zamawiający wymaga jej dostarczenia. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz FC - licencje na protokoły CIFS, NFS, FCP oraz iSCSI są przedmiotem obecnego postępowania. |
|  | Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania, ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, etc. |
|  | System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru plikowych wolumenów danych: (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych |
|  | Musi być możliwość konfiguracji macierzy dyskowej za pomocą GUI, zbieranie i wyświetlanie informacji o stanie zasobów macierzy dyskowej, prezentowanie i gromadzenie zdarzeń zachodzących w macierzy dyskowej oraz prezentowanie bieżących statystyk wydajnościowych macierzy dyskowej, podgląd parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym. |
|  | Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego. |
|  | W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft Active Directory. |
|  | W celu zabezpieczania danych macierz dyskowa musi posiadać licencję, która umożliwi wykonywanie replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy i pracować w trybie asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gatawey, serwer pośredniczący, etc. Musi istnieć możliwość odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być zrealizowana zewnętrznym narzędziem software'owym. Licencja na replikację jest przedmiotem obecnego postępowania. |
|  | System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub analogicznych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu. |
|  | Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy. |
|  | Wymagana jest możliwość replikacji dwukierunkowej (bi-directional). |
|  | Wymagana jest funkcjonalność kompresji i deduplikacji danych wysyłanych po sieci WAN. |
|  | Testy przywracania danych (Data Recovery) muszą być możliwe bez konieczności zmian w działaniu replikacji (np. PAUSE, REVERSE). |
|  | Oprogramowanie musi mieć możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK. |
|  | Wymagana jest możliwość ciągłego wykonywania kopii (bez wykorzystania mechanizmu kopii migawkowych VMware) podczas pracy maszyny wirtualnej. |
|  | Wymagane jest RPO na poziomie pojedynczych sekund. |
|  | Wymagana jest możliwość wyboru dowolnego punktu w czasie (z ostatnich 5 dni), z którego chcemy odtworzyć dane lub całe środowisko. |
|  | Wymagana jest możliwość przeprowadzania testów DR bez zatrzymywania przetwarzania produkcyjnego. |
|  | Wymagana jest możliwość tworzenia własnych scenariuszy odtwarzania w przypadku awarii. |
|  | Oprogramowanie musi mieć możliwość automatycznego wykonywania kopii maszyn wirtualnych pracujących w środowisku wykorzystującym technologie VMware VMotion, VMware S-VMotion, VMware DRS, VMware HA. |
|  | Oprogramowanie musi być odporne na krótkotrwałe problemy (np. przerwy w dostępności) związane z siecią WAN. |
|  | Oprogramowanie musi być odporne na zmiany sprzętowe środowiska (zmiany w warstwie sprzętowej nie mogą mieć negatywnego wpływu na działanie systemu). |
|  | Oprogramowanie musi posiadać pełną redundancję bez pojedynczego punktu awarii. |
|  | Jeżeli pełna redundancja nie jest możliwa na poziomie samej aplikacji należy zaimplementować tą funkcjonalność na poziomie VMware. |
|  | Koszty takiego rozwiązania muszą być uwzględnione w ofercie (licencje i usługi).  Oprogramowanie musi posiadać mechanizm synchronicznej replikacji między lokalizacjami dla krytycznych maszyn VM. |
|  | Jeżeli replikacja synchroniczna nie jest możliwa za pomocą tej samej aplikacji Wykonawca musi dostarczyć dodatkowe rozwiązanie do replikacji synchronicznej wybranych maszyn VM (ok. 40 maszyn). |
|  | Oprogramowanie musi zapewnić następującą retencję przechowywanych kopi bezpieczeństwa:   * RPO = 30s z ostatnich 24h, * RPO = 24h z ostatniego tygodnia, * RPO = 1 tydzień z ostatniego miesiąca |
|  | Dopuszcza się zastosowanie uzupełniającego oprogramowanie backupowego do składowania danych z dłuższą retencją. |
|  | Oba systemy replikacji muszą działać jednocześnie i być kompatybilne. |
|  | Wymagana jest możliwość zarządzania oprogramowaniem z poziomu vCenter. |
|  | Wymagane jest wsparcie dla wykonywania kopii maszyn wirtualnych z systemów VMware w wersji 6.0 i nowszych. |
|  | Macierz wyposażona w ponad 256GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. |
|  | Możliwość instalacji więcej niż 24 dyski 2,5” w obudowie kontrolera. Macierz nie zajmuje więcej niż 2U w szafie RACK. Możliwość rozbudowy macierzy o półki dyskowe umożliwiające instalację dysków SSD, SAS i NL\_SAS w tej samej półce dyskowej. |
|  | Wymagania gwarancyjne. Macierz i wszystkie zaoferowane podzespoły muszą być objęte gwarancją na okres 60 miesięcy, czas naprawy Następny Dzień Roboczy. Uszkodzone dyski pozostają własnością Zamawiającego. |

## Urządzenia sieciowe

### Urządzenie sieci LAN, przełącznik – 2 szt.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
|  | Przełącznik 1U wyposażony w porty/interfejsy:  - 48 x 10 Gigabit Ethernet Base-T.  - 6 x 40 Gigabit Ethernet QSFP+  - 1 x RJ45 console/management port with RS232 signaling  - 1 x USB 2.0 type A to support mass storage device  - 1 x Micro-USB 2.0 type B Serial Console Port  Musi umożliwiać obsługę wszystkich portów line-rate, z jednoczesną możliwością instalacji modułów SFP w miejsce portów 10 Gigabit Ethernet   * Musi posiadać gniazdo dla opcjonalnego modułu łączenia w stos lub możliwość zestawienia stosu portami 40GbE (do min 6 urządzeń) |
|  | Przełącznik musi umożliwiać przepustowość zagregowaną minimum 1080 Mpps, |
|  | Przełącznik musi posiadać modularny system operacyjny. |
|  | Przełącznik musi umożliwiać instalacje różnych systemów operacyjnych wspieranych przez producenta w celu uzyskania dodatkowych funkcjonalności zgodnie z rekomendacją SDN. |
|  | Przełącznik musi posiadać nadmiarowy zasilacz AC (hot-swapable), Max. konsumpcja mocy: 420 Watts. |
|  | Przełącznik musi być dostosowany do instalacji w szafach 19” |
|  | Przełącznik musi posiadać moduły pamięci SSD: 8 GB Pamięć CPU: 4GB Pojemność bufora pakietów: 16MB |
|  | Przełącznik musi istnieć możliwość zamiany interfejsów 40 Gigabit Ethernet na 4 x 10Gigabit Ethernet SFP+ lub równoważne za pomocą kabli rozszywających.  Wymagana obsługa min. 72 portów 10Gigabit Ethernet line-rate na przełącznik z wykorzystaniem kabli rozszywających. |
|  | Przełącznik musi posiadać matrycę przełączającą o wydajności min. 1.44Tbps (full-duplex); |
|  | Szybkość przełączania ramki w obrębie przełącznika maksymalnie 2.5 us mikro sekund; |
|  | Przełącznik musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne). |
|  | Przełącznik musi być wyposażony w redundantne i wymienne w trakcie pracy (hot-swappable) 2 wiatraki. |
|  | Musi obsługiwać ramki „Jumbo” o długości min. 11000 B.  Musi obsługiwać, co najmniej 4000 VLANów.  Musi posiadać pamięć, dla co najmniej 160 000 adresów MAC.  Musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+, MSTP  Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach  - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy  - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń  - implementacje dedykowanego protokołu innego niż STP, RSTP, PVST+, MSTP umożliwiający szybką konwergencję sieci w przypadku zastosowania topologii Ring.  Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG  Musi obsługiwać DCB (Data Center Bridging)  Musi zapewniać sprzętowe wsparcie dla L3 VXLAN routing line rate L3  Musi obsługiwać protokół Ethernet Ring Protection Switching, (ERPS) lub równoważny |
|  | Przełącznik musi obsługiwać standardy IEEE:  802.1AB LLDP  802.1ag Connectivity Fault Management  802.1D Bridging, STP  802.1p L2 Prioritization  802.1Q VLAN Tagging, Double VLAN Tagging, GVRP  802.1X Network Access Control (Port Authentication)  802.3ab Gigabit Ethernet (1000BASE-T)  802.3ac Frame Extensions for VLAN Tagging  802.3ad Link Aggregation with LACP  802.3ae 10 Gigabit Ethernet (10GBASE-X)  802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4)  802.3u Fast Ethernet (100BASE-FX) on management ports  802.3x Flow Control  802.3z Gigabit Ethernet (1000BASE-X)  ANSI/TIA-1057 LLDP-MED. |
|  | Przełącznik musi obsługiwać, co najmniej poniższe standardy:  768 User Datagram Protocol  793 Transmission Control Protocol  854 Telnet Protocol Specification  959 File Transfer Protocol (FTP)  1321 The MD5 Message-Digest Algorithm  1350 The TFTP Protocol (Revision 2)  2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers  3164 The BSD syslog Protocol  5880 Bidirectional Forwarding Detection |
|  | Przełącznik musi obsługiwać co najmniej poniższe standardy RFC w zakresie protokołu IPv4:  791 Internet Protocol  792 Internet Control Message Protocol  826 An Ethernet Address Resolution Protocol  1027 Using ARP to Implement Transparent Subnet Gateways  1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION (client)  1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks  1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis  1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy  1542 Clarifications and Extensions for the Bootstrap Protocol  1812 Requirements for IP Version 4 Routers  1858 IP Fragment Filtering  2131 Dynamic Host Configuration Protocol  2338 Virtual Router Redundancy Protocol (VRRP)  3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links  3046 DHCP Relay Agent Information Option  3069 VLAN Aggregation for Efficient IP Address Allocation  3128 Protection Against a Variant of the Tiny Fragment Attack |
|  | Przełącznik musi obsługiwać, co najmniej poniższe standardy RFC w zakresie protokołu IPv6:  1858 IP Fragment Filtering  2460 Internet Protocol, Version 6 (IPv6) Specification  2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification  2675 IPv6 Jumbograms  3587 IPv6 Global Unicast Address Format  4291 Internet Protocol Version 6 (IPv6) Addressing Architecture  Musi obsługiwać Multicast w tym, co najmniej poniższe standardy RFC i drafty:  1112 Host Extensions for IP Multicasting  2236 Internet Group Management Protocol, Version 2  3376 Internet Group Management Protocol, Version 3  3569 An Overview of Source-Specific Multicast (SSM)  4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches  draft-ietf-pim-sm-v2-new-05 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)  Musi umożliwiać obsługę Statycznego i Dynamicznego Routingu:  W tym co najmniej poniższe standardy RFC dla OSFP:  1587 The OSPF Not-So-Stubby Area (NSSA) Option  2154 OSPF with Digital Signatures  2328 OSPF Version 2  2370 The OSPF Opaque LSA Option  3623 Graceful OSPF Restart  4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance  W tym co najmniej poniższe standardy RFC i drafty dla BGP:  1997 BGP Communities Attribute  2385 Protection of BGP Sessions via the TCP MD5 Signature Option  2439 BGP Route Flap Damping  2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing  2796 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)  2842 Capabilities Advertisement with BGP-4  2858 Multiprotocol Extensions for BGP-4  2918 Route Refresh Capability for BGP-4  3065 Autonomous System Confederations for BGP  4360 BGP Extended Communities Attribute  4893 BGP Support for Four-octet AS Number Space  5396 Textual Representation of Autonomous System (AS) Numbers  draft-ietf-idr-bgp4-20 Border Gateway Protocol 4 (BGP-4)  draft-ietf-idr-restart-06 Graceful Restart Mechanism for BGP  **W tym, co najmniej poniższe standardy RFC dla IS-IS:**  1195 Routing in TCP/IP and Dual Environments  5308 Routing IPv6 with IS-IS  **W tym, co najmniej poniższe standardy RFC dla VRF**:  4364 VRF-lite (IPv4 VRF with OSPF, BGP, IS-IS and V4 multicast) |
|  | Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:   * Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, * Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. * Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). * Implementacja mechanizmu Weighted Random Early Detection (WRED). * Obsługa IP Precedence i DSCP |
|  | Przełącznik musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci:   * Co najmniej 3 poziomy dostępu administracyjnego przez konsole: * Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100/1000BaseT * Autoryzacja użytkowników/portów w oparciu o 802.1x oraz EAP * Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2 * Implementacji listy kontroli dostępu (ACL) na poziomie co najmniej warstwy 2 * Obsługa DHCP Snooping * Obsługa dynamicznej inspekcji ARP * Obsługa walidacji adresów IP o MAC (MAC+IP Source Address Validation) * Obsługa walidacji adresów MAC (DHCP MAC Address Validation) * Obsługa, co najmniej sFlow v5 lub ekwiwalentu * Obsługa RMON * Obsługa monitorowania ruchu na porcie (Port Monitoring) * Plik konfiguracyjny urządzenia musi być możliwy do edycji ‘off-line’. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian. |
|  | Przełącznik musi posiadać funkcjonalność automatycznej konfiguracji poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware) i pliku konfiguracyjnego w trakcie pierwszego podłączenia do sieci Ethernet |
|  | 5 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do końca następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat. |
|  | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# SYSTEM KOPII BEZPIECZEŃSTWA

Systemu Kopii Bezpieczeństwa dla powstałej w Zamówieniu infrastruktury powinien zakładać, że całe środowiska Podstawowe i Zapasowe oparte są o platformę wirtualizacją będącą elementem tego Zamówienia przy 100% wypełnieniu danymi. W skład Systemu Kopii Bezpieczeństwa powinno wchodzić urządzenie do deduplikacji danych wraz z oprogramowaniem pozwalającym na konfiguracje i zarzadzanie środowiskiem backupów, które będzie funkcjonować w Środowisku Podstawowym. W Środowisku Zapasowym zostanie wdrożone rozwiązanie programowe, działające w ramach dostępnej wirtualizacji, umożliwiające na replikację danych z urządzenia do deduplikacji w Środowisku Podstawowym oraz odtworzenie ich na wypadek awarii Środowiska Podstawowego.

Wykonawca musi dostarczyć rozwiązane SKB kompatybilne z platformą wirtualizacją posiadaną przez Zamawiającego oraz tą która zostanie dostarczona w ramach Zamówienia jak również z oprogramowaniem:

* MS SQL 2008 i nowszych
* Windows 2008/Windows 2008 R2/MS Windows 2012,
* Linux,
* usługi katalogowe system MS Windows 2003 i nowszymi.
* MS Exchange 2016 pozwalającego backup’ować serwer pocztowy bez konieczności jego wyłączania oraz z możliwością kopiowania i odzyskiwania z dokładnością do jednego lub kilku wskazanych konta.

Systemy podlegające procedurze kopii bezpieczeństwa (maszyny wirtualne) wraz z procedurami zostanie ujęty w Projekcie Technicznym.

## Wymagania dotyczące Systemu Kopii Bezpieczeństwa (SKB)

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
|  | Urządzenie musi być przeznaczone do de-duplikacji, dedykowane do przechowywania kopii zapasowych. |
|  | Urządzenie będące przedmiotem zapytania musi oferować przestrzeń 14TB netto (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do 170TB powierzchni netto w ramach tego samego urządzenia. Rozbudowa do wymaganej pojemności powinna być możliwa poprzez dołożenie kolejnych półek z dyskami oraz odpowiednich licencji, rozbudowa nie może pociągać konieczności dołożenia dodatkowych kontrolerów, nie może być również realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń. |
|  | Oferowane urządzenie musi posiadać minimum:   * 4 porty Ethernet 10 Gb/s RJ45 - wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle; * 4 porty Ethernet 10 Gb/s OP – wymagana możliwość obsługi każdym z portów protokołów CIFS, NFS, de-duplikacja na źródle; |
|  | Oferowane urządzenie musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami czyli dla Ethernet:   * CIFS, NFS, deduplikacja na źródle (alternatywnie OST/BOOST/CATALYST)   oraz jednocześnie dla FC (po dodaniu odpowiednich portów)   * VTL, de-duplikacja na źródle (alternatywnie OST/BOOST/CATALYST)   w obrębie oferowanej pojemności urządzenia. |
|  | Wymagane jest dostarczenie licencji pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, VTL w przypadku pojemności oferowanego urządzenia na poziomie 170TB netto co oznacza, że rozbudowa urządzenia z wymaganych 14TB netto do 170TB netto nie może pociągać konieczności dodania kolejnych licencji w przypadku wykorzystywania protokołów CIFS, NFS, VTL w obrębie wymaganej maksymalnej pojemności urządzenia. |
|  | Wymagane jest dostarczenie licencji zapewniających funkcjonalność: blokada skasowania danych w obrębie maksymalnej wymaganej pojemności urządzenia.  Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem bądź modyfikacją.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):   1. umożliwiającym zdjęcia blokady przed upływem ważności danych 2. nieumożliwiającym zdjęcia blokady przed upływem ważności danych (compliance) |
|  | Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia. |
|  | Wymaga się aby pojedyncze urządzenie dla maksymalnej pojemności (170TB netto) osiągało zagregowaną wydajność w przypadku protokołów CIFS, NFS na poziomie co najmniej 8 TB/h (dane podawane przez producenta w ogólnie dostępnych dokumentach) oraz co najmniej 24 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta w ogólnie dostępnych dokumentach). |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 270 strumieni w tym jednocześnie:   * zapis danych minimum 150 strumieniami * odczyt danych minimum 70 strumieniami * replikacja minimum 50 strumieniami   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 270 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu, jednocześnie 70 strumieni dla odczytu oraz jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line). |
|  | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4, LTO5. |
|  | Urządzenie musi umożliwiać jednoczesną emulację min. 250 napędów oraz 60 000 slotów w przypadku trybu VTL. |
|  | Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
|  | Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
|  | Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. |
|  | De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jakie są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia w celu maksymalnego zwiększenia efektywności deduplikacji. |
|  | Niedopuszczalna jest de-duplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest kazdy strumień danych. |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia.  W obrębie całego urządzenia, raz otrzymany i zapisany w urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. |
|  | Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych. |
|  | Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być kompresowane. |
|  | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: HP Data Protector, IBM TSM, VERITAS NetBackup, EMC Networker, Oracle RMAN, IBM BRMS, IBM Data Studio, SAP BR\*Tools, SAP HANA Studio, Microsoft SQL Server Management Studio, Veeam. |
|  | W przypadku współpracy z każdą z poniższych aplikacji:   * RMAN (dla ORACLE) * Microsoft SQL Server Management Studio (dla Microsoft SQL) * IBM Data Studio (dla DB2) * SAP BR\*Tools (dla SAP/Oracle) * SAP HANA STUDIO (dla SAP HANA) * VERITAS NetBackup * HP Data Protector * EMC NetWorker * Veeam   Urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do oferowanego urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | W przypadku przyjmowania backupów z VERITAS NetBackup, EMC NetWorker, Oracle RMAN, Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio) , IBM DB2 (przy wykorzystaniu IBM Data Studio), SAP/Oracle (przy wykorzystaniu SAP BR\*Tools), SAP HANA (przy wykorzystaniu SAP HANA STUDIO), Veeam urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC (po doposażeniu urządzenia w odpowiednie porty).  De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
|  | Urządzenie musi wspierać de-duplikację na źródle w sieci FC (SAN) minimum dla następujących systemów operacyjnych:   * Windows * Linux (RedHat, SuSE) * HP-UX * AIX * Solaris |
|  | Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane z poziomu aplikacji VERITAS NetBackup, EMC NetWorker |
|  | Urządzenie powinno dopuszczać co najmniej 90% utylizację powierzchni netto, bez widocznego spadku wydajności. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy czy obostrzenia, które mogą pojawić się przy zapełnieniu urządzenia poniżej 90%. |
|  | Urządzenie musi również umożliwiać wydzielenie określonych portów Ethernet do replikacji. |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
|  | W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy VERITAS NetBackup / HP Data Protector /EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu   replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
|  | Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%. |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. |
|  | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID |
|  | Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare. |
|  | Oferowane urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania). |
|  | Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie. |
|  | Urządzenie musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia). |
|  | Urządzenie musi mieć możliwość podziału na minimum 14 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 14 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
|  | Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego poprzez:   * CIFS * NFS * VTL   Zamawiający wymaga protokół umożliwiający deduplikację na źródle. |
|  | Urządzenie musi weryfikować wszystkie zabezpieczane dane podczas procesu zapisu (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie, opisana funkcjonalność powinna być częścią procesu zapisywania danych co oznacza, że weryfikacja realizowana podczas produkcyjnego dostępu do danych (w trakcie procesu RESTORE) a nie podczas procesu zapisu danych na urządzeniu - nie spełnia niniejszych wymagań. Powyższa weryfikacja musi odbywać się w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). |
|  | Wymagana możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). |
|  | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie może być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
|  | Urządzenie musi mieć możliwość zarządzania poprzez   * interfejs graficzny dostępny z przeglądarki internetowej * poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
|  | Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
|  | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Urządzenie musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postepowania. |
|  | Wymagane wsparcie realizowane przez producenta na okres min. 5 lat w trybie 5x9 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania sprzętowego. |

# ŚWIADCZENIE USŁUGI SERWISU I GWARANCJI

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis funkcjonalności** |
| WUS.1 | Wykonawca będzie przyjmował zgłoszenia o Incydentach serwisowych w trybie **24 godziny na dobę 7 dni** **w tygodniu**. |
| WUS.2 | W celu zarządzania Incydentami serwisowymi Wykonawca zapewni system do obsługi Incydentów serwisowych, za pomocą, którego dokonywane będą zgłoszenia Incydentów serwisowych, obsługa i monitorowanie Incydentów serwisowych (np. system oparty na komunikacji za pomocą poczty elektronicznej ze zgłaszającym Incydent serwisowy lub zakładający interakcję ze zgłaszającym Incydent serwisowy, za pomocą graficznego interfejsu użytkownika lub stanowiący połączenie obydwu ww. form). |
| WUS.2.1 | Wykonawca umożliwi przyjęcie i obsługę Incydentów serwisowych kierowanych faksem lub mailem na adres podany przez Wykonawcę. |
| WUS.3 | Po wymianie Urządzenia lub modułu będącego wyposażeniem tego Urządzenia lub Oprogramowania zostanie on objęty serwisem na takich samych zasadach jak wymienione Urządzenie lub moduł będący wyposażeniem tego Urządzenia lub Oprogramowania. |
| WUS.4 | Usunięcie Błędu zostanie zakończone przywróceniem działania Urządzenia lub Oprogramowania sprzed Błędu. |
| WUS.5 | Wykonawca najpóźniej w 1 Dzień Roboczy, po rozwiązaniu Incydentu serwisowego przedstawi raport z tego Incydentu serwisowego (prezentujący, co najmniej czasy przyjęcia zgłoszenia o Incydencie serwisowym oraz rozwiązania Incydentu serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Incydentu serwisowego). |
| WUS.6 | Do każdego dostarczonego Urządzenia lub Oprogramowania Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną producenta, zawierającą numer seryjny, termin i warunki ważności gwarancji. Jeśli dla danego dostarczonego Urządzenia lub Oprogramowania producent nie przewiduje wystawiania własnych kart gwarancyjnych, kartę taką wystawi Wykonawca. W celu ułatwienia Zamawiającemu zarządzania kartami gwarancyjnymi dopuszcza się wystawianie zbiorczych kart gwarancyjnych Wykonawcy, jednakże każdorazowo z podaniem nr seryjnych lub innych danych umożliwiających jednoznaczną identyfikację Urządzenia lub Oprogramowania, którego dotyczy gwarancja Wykonawcy. W wypadku, jeżeli postanowienia gwarancji producenta są mniej korzystne od warunków zapisanych w Umowie, stosuje się zapisy Umowy. |
| WUS.7 | W przypadku zgłoszeń serwisowych niemieszczących się w zakresie świadczonych usług wynikających z niniejszego zamówienia, Wykonawca zobowiązany jest  do przekierowania zgłoszenia serwisowego do odpowiedniego podmiotu na zasadach określonych przez Zamawiającego. |
| WUS.8 | Gwarancja na dostarczone Urządzenia i Oprogramowanie biegnie osobno dla każdego z ww. urządzeń / oprogramowania, od dnia podpisania Protokołu Odbioru Urządzeń – odnośnie Urządzeń i Oprogramowania Standardowego dostarczonych Zamawiającemu w ramach Etapu 1, zaś od dnia podpisania Protokołu Odbioru Etapu 2 – w pozostałym zakresie, w tym dla Uzupełnień i Oprogramowania przekazanych Zamawiającemu w ramach Etapu 2, przez okres 60 miesięcy od podpisania protokołu odbioru Etapu 2. W przypadku, jeżeli świadczenie gwarancyjne polegać będzie na wymianie wadliwego Urządzenia lub modułu będącego wyposażeniem tego Urządzenia lub Oprogramowania na wolne od wad, okres gwarancji dla tego Urządzenia lub modułu będącego wyposażeniem tego Urządzenia lub Oprogramowania biegł będzie od daty protokołu stwierdzającego tę wymianę, przez okres standardowo udzielany przez producenta, lecz nie krócej niż do dnia Gwarancji udzielanej przez Wykonawcę na Uzupełnienia, na warunkach określonych w Umowie. |
| WUS.9 | Wykonawca dokona usunięcia Błędu Niekrytycznego w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia Błędu Niekrytycznego (usunięcie Błędu Niekrytycznego rozumiane jest, jako przywrócenie funkcjonalności Systemu sprzed Błędu Niekrytycznego). |
| WUS.10 | Wykonawca dokona usunięcia Błędu Zwykłego w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia Błędu Zwykłego (usunięcie Błędu Zwykłego rozumiane jest, jako przywrócenie funkcjonalności Systemu sprzed Błędu Zwykłego). |
| WUS.11 | Wykonawca dokona naprawy (lub wymiany) Urządzenia w Lokalizacji wskazanej przez Zamawiającego; w przypadku konieczności dokonania naprawy poza Lokalizacją, w której zainstalowany zostanie System, Wykonawca pokryje koszty transportu oraz koszty ewentualnego ubezpieczenia przedmiotu zamówienia do miejsca naprawy oraz jego zwrotu do Lokalizacji. |
| WUS.12 | W przypadku, gdy wadliwe Urządzenie uniemożliwia wykorzystanie funkcjonalności Systemu lub uniemożliwia pracę jakiegokolwiek jego podsystemu Wykonawca  na czas naprawy zobowiązany jest dostarczyć, skonfigurować i uruchomić urządzenie zastępcze w sposób, który pozwoli na przywrócenie utraconych funkcjonalności Systemu lub podsystemu. |
| WUS.13 | Przez usunięcie Błędów rozumie się rozwiązanie problemu albo zaproponowanie procedury obejścia zaistniałych Błędów bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę. |
| WUS.14 | Wykonawca jest zobowiązany do samodzielnego dokonania naprawy/wymiany Urządzenia w Lokalizacji. Jednakże, o ile Zamawiający wyrazi uprzednią zgodę, dopuszcza się realizację świadczenia gwarancyjnego w ten sposób, że na podstawie informacji diagnostycznych przekazanych przez Zamawiającego do Wykonawcy podczas zgłoszenia Błędów, Wykonawca prześle na swój koszt zamiennik uszkodzonego Urządzenia, natomiast fizycznej wymiany uszkodzonego Urządzenia dokona odpowiednio przeszkolony przez Wykonawcę pracownik Zamawiającego, czyniąc to na ryzyko Wykonawcy. Jednakże taki tryb realizacji naprawy nie zwalnia Wykonawcy z obowiązku zapewnienia przywrócenia pierwotnego stanu pracy Systemu. |
| WUS.15 | Gwarancja obejmuje również wykonanie przez Wykonawcę wszelkich czynności związanych z przywróceniem pierwotnego stanu pracy Systemu (sprzed Błędu) oraz pokrycie przez Wykonawcę kosztów części zamiennych użytych do przywrócenia Systemu do stanu pierwotnego (sprzed Błędu). |
| WUS.16 | W okresie udzielenia gwarancji na Oprogramowanie Standardowe Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania Standardowego do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware), patch’y, programów korekcji wszelkich błędów (w szczególności Błędów Krytycznych, Błędów Zwykłych, Błędów), a także dostęp do usług wsparcia technicznego producenta danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu wymagane informacje umożliwiające Zamawiającemu dostęp do usług wsparcia technicznego producenta oraz aktualizacji w okresie gwarancji, a także każdorazowo w przypadku zmian informacji przekazanych Zamawiającemu.  Zamawiający wymaga od Wykonawcy realizacji w ramach Umowy, w tym w okresie gwarancji, prac związanych z dostosowaniem i przetestowaniem Systemu do przedmiotowych aktualizacji Oprogramowania Standardowego (włączając tzw. firmware). |
| WUS.17 | Zamawiający zastrzega sobie prawo do dodawania nowych modułów dowolnych producentów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. |
| WUS.18 | Gwarancja obejmuje między innymi:   * + wady materiałowe i konstrukcyjne, a także nie spełnienie deklarowanych przez producenta parametrów i/lub funkcji użytkowych Urządzeń i Oprogramowania;   + naprawę wykrytych uszkodzeń, w tym wymianę uszkodzonych modułów na nowe;   + usuwanie wykrytych usterek i Błędów w działaniu Urządzeń lub Oprogramowania. |
| WUS.19 | W przypadku Błędu dysku twardego, powodującej konieczność jego wymiany, uszkodzony dysk pozostanie u podmiotu, który posiada uprawnienia do korzystania z Urządzeń i Oprogramowania dostarczonego w ramach realizacji niniejszej Umowy oraz nie będzie podlegał ekspertyzie poza siedzibą. W przypadku konieczności jakiejkolwiek naprawy sprzętu poza miejscem jego instalacji, dysk twardy zostanie zdemontowany i pozostanie w Lokalizacji jego użytkowania. |
| WUS.20 | Dwukrotne uszkodzenie tego samego Urządzenia lub modułu będącego wyposażeniem tego Urządzenia w okresie gwarancji, obliguje Wykonawcę do jego wymiany na fabrycznie nowy, wolny od wad, spełniający te same parametry i zgodny funkcjonalnie z naprawianym Urządzeniem, w terminie 14 dni od chwili ostatniego zgłoszenia o uszkodzeniu. Okres gwarancji na wymienione Urządzenie biegł będzie od daty protokołu stwierdzającego tę wymianę, przez okres standardowo udzielany przez producenta, lecz nie krócej niż do dnia Gwarancji udzielanej przez Wykonawcę na Uzupełnienia, na warunkach określonych w Umowie. |
| WUS.21 | Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie Systemu. |
| WUS.22 | Gwarantowany czas naprawy szczególnych elementów zamawiający określa w ramach wymogów poszczególnych składników Systemu |

# WYMAGANIA DOTYCZĄCE USŁUGI INSTALACJI URZĄDZEŃ.

- minimalne wymagania dla usługi instalacji Urządzeń

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDRU.1 | Usługi instalacyjne muszą obejmować w szczególności:   * Dostarczenie Urządzeń do wskazanych przez Zamawiającego Lokalizacji; * Rozpakowanie Urządzeń oraz utylizacja/magazynowanie opakowań; * Montaż Urządzeń w posiadanych przez Zamawiającego szafach; * Podłączenie Urządzeń do zapewnianych przez Zamawiającego obwodów zasilających; * Instalacja Urządzeń zgodnie z Projektem Technicznym Uzupełnień; * Instalacja Oprogramowania na Urządzeniach; * Konfiguracja Urządzeń; * Uruchomienie Urządzeń. |
| WDRU.2 | Usługi konfiguracyjne muszą obejmować w szczególności:   * Konfigurację Urządzeń oraz Oprogramowania zgodnie z Projektem Technicznym Uzupełnień, |
| WDRU.3 | Usługi testowe muszą zostać przeprowadzone zgodnie z procedurą określoną w Planie Testów Akceptacyjnych, dokumencie opracowanym przez Wykonawcę zgodnie z wymaganiem DOK.1.1.2 |
| WDRU.3.1 | Zamawiający zastrzega sobie prawo do zlecenia wykonania całości lub części testów przez wskazany przez niego podmiot zewnętrzny. |
| WDRU.4 | Usługi wdrożeniowe muszą obejmować w szczególności:   * Uruchomienie Systemu będącego przedmiotem zamówienia w celu przeprowadzenia testów akceptacyjnych zgodnie z Planem Wdrożenia Systemu, * Przekazania rozwiązania produkcyjnego Zamawiającemu, * Wykonanie Dokumentacji Powykonawczej zawierającej szczegółowy opis wdrożonego rozwiązania oraz zmian w dokumentacji projektowej uwzględniającej poprawki naniesione w trakcie wdrożenia. |

# MINIMALNE WYMAGANIA W ZAKRESIE USŁUGI WDROŻENIA.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDUK.1 | Wykonawca wykona integrację dostarczonego rozwiązania z system monitorowania zasobów Zabbix 3.4, użytkowanego przez Zamawiającego, w ramach wspieranych metod przez to oprogramowanie (SNMPv2, SNMPv3, JMX, IPMI, Zabbix Agent). Zamawiający oczekuje, że wszystkie komponenty sprzętowe oraz oprogramowanie, które mają możliwość monitorowania w ramach protokołów wspieranych przez system Zabbix, zostaną podłączone. Integracja będzie polegała na:   * Konfiguracji urządzeń lub/i oprogramowania pozwalającą na poprawną pracę * Konfiguracji konfiguracji oprogramowania Zabbix, a w szczególności reguł wykrywania, szablonów i wyzwalaczy. |
| WDUK.2 | Zamawiający wymaga aby wszelkie oprogramowanie do zarządzania, wchodzące w skład rozwiązania a musi być zainstalowane na wskazanym przez Zamawiającego serwerze. |
| WDUK.3 | W ramach wdrożenia zostanie wyodrębnione środowisko zapasowe (z aktualnych elementów infrastruktury Zamawiającego) i środowisko produkcyjne (powstałe z dostarczonych elementów w ramach Zamówienia). Pomiędzy Środowiskiem Podstawowym i Zapasowym musi być uruchomiona replikacja danych w ramach sprzętowego deduplikatora w Środowisku Podstawowym a wirtualnym rozwiązaniem deduplikatora w Środowisku Zapasowym. |
| WDUK.4 | Wdrożone rozwiązanie powinno umożliwiać przeniesienie środowiska zapasowego w inną lokalizację fizyczną przy zastosowaniu połączeń VPN w ramach posiadanych przez Zamawiającego urządzeń. |
| WDUK.5 | W ramach wdrożenia, Wykonawca skonfiguruje nowe środowisko produkcyjne do aktualnie funkcjonującej struktury sieci Zamawiającego. |
| WDUK.6 | W ramach wdrożenia, Wykonawca przeniesie aktualne środowisko wirtualne do nowej infrastruktury. Migracja, musi być wykonana w taki sposób aby zapewnić ciągłość działania usługaktualnego Środowiska Podstawowego. Wykonawca zaproponuje w Projekcie Technicznm najlepszą metodę przeniesienia środowiska wirtualnego, która pozwoli na jak najkrótszy przestój. Wszelkie praca, powodujące przestój Systemów Zamawiającego winny być wykonywane w weekendy, w godzinach nocnych. |
| WDUK.7 | Wykonawca zaprojektuje i wdroży rozwiązanie realizujące automatyczne próby odzyskiwania z backupów (testy odtworzeniowe). |
|  | Oczekujemy, aby środowisko zapasowe umożliwiało awaryjne uruchomienie z backupu maszyn w przypadku awarii infrastruktury produkcyjnej. |
| WDUK.8 | Konfiguracja kopii bezpieczeństwa środowiska zapasowego w ramach. |
| WDUK.9 | Wykonawca dokona niezbędnej adaptacji i rekonfiguracji sieci Środowiska Podstawowego oraz Środowiska Zapasowego w oparciu o posiadane przez Zamawiającego sprzęt i zasoby sieciowe. |

# WYMAGANIA W ZAKRESIE WARSZTATÓW.

W ramach indywidualnych Zleceń Wykonawca każdorazowo przeprowadzi warsztaty tematycznew zakresie dostarczanych rozwiązań w niniejszym zamówieniu, zgodnie z poniżej przedstawionymi wymaganiami:

- minimalne wymagania w zakresie warsztatów.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis funkcjonalności** |
| WRT.1 | Wykonawca przeprowadzi warsztaty w języku polskim, obejmujące wykłady teoretyczne oraz warsztaty praktyczne w zakresie administrowania rozwiązaniami dostarczonymi w niniejszym zamówieniu (w tym wykonanie wybranych przez Zamawiającego procedur dostarczanych w ramach niniejszego zamówienia). Warsztaty będą się odbywać w siedzibie Zamawiającego.  Warsztaty muszą swoją tematyką objąć co najmniej następujące tematy:   * + Administrowanie Systemem Kopii Bezpieczeństwa   + Administrowanie Systemem Wirtualizacji.   + Zarządzanie urządzeniami sieciowymi.   + Zarządzanie i utrzymanie sprzętu dostarczonego w ramach Zamówienia. |
| WRT.2 | Wykonawca w ramach Etapu 2 opracuje i dostarczy Zamawiającemu Opis Realizacji Warsztatów zawierający:   * cel i projektowany zakres warsztatów, * metodę i formę warsztatów, * podział na dzienne bloki tematyczne warsztatów, * opis dziennych bloków tematycznych (minimum 5 bloków) * wykaz pożądanych kwalifikacji osób skierowanych na warsztaty, * koszt osobowy udziału uczestnika w jednym bloku warsztatów * sposób weryfikacji zdobytej przez uczestników wiedzy. |
| WRT.3 | Opis Realizacji Warsztatów, o którym mowa w wymaganiu WRT.2, Wykonawca  przedstawi do akceptacji Zamawiającego. |
| WRT.4 | Wykonawca zobowiązany jest do przeprowadzenia warsztatów każdorazowo zgodnie ze Zleceniem na podstawie zatwierdzonego przez Zamawiającego Opisu Realizacji Warsztatów, o którym mowa w wymaganiu WRT.2. |
| WRT.5 | Zamawiający wymaga realizacji przez Wykonawcę warsztatów na podstawie Zleceń, dla łącznej grupy uczestników do **2 osób** wskazanych przez Zamawiającego. |
| WRT.6 | Wykonawca zapewni materiały warsztatowe (w języku polskim) dla uczestników warsztatów oraz przeniesie prawa autorskie do opracowanych przez Wykonawcę materiałów warsztatowych. |
| WRT.7 | Wykonawca zapewni prowadzenie warsztatów przez wykwalifikowaną kadrę posiadającą wiedzę teoretyczną i praktyczną w zakresie użytkowania i administrowania rozwiązaniami dostarczanymi w ramach niniejszego zamówienia. |
| WRT.8 | Przeprowadzenie warsztatów zostanie potwierdzone protokołem sporządzonym w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:   * nazwę i tematykę i czas trwania warsztatów, * datę i miejsce warsztatów, * imienną listę osób podpisaną przez uczestniczących w warsztatach, * imię i nazwisko oraz specjalizację osób prowadzących warsztaty. |
| WRT.11 | Odbiór warsztatów nastąpi na podstawie protokołu odbioru Zlecenia dot. warsztatów, na podstawie którego warsztat został przeprowadzony, podpisanego przez Zamawiającego bez uwag i zastrzeżeń. |
| WRT.14 | Czas trwania warsztatów wyniesie maksymalnie 2 dni po 8 godzin dziennie dla każdego uczestnika warsztatów. |
| WRT.15 | Wykonawca zapewni materiały warsztatowe każdemu uczestnikowi warsztatów, od momentu rozpoczęcia warsztatów, zarówno w formie papierowej jak i elektronicznej formie niezabezpieczonej (w formacie .pdf, .doc, .docx, .pps, ppsx). |
| WRT.16 | Warsztaty będą realizowane każdorazowo na podstawie Zleceń w siedzibie Zamawiającego. |
| WRT.17 | Zlecenie realizacji warsztatów przez Zamawiającego jest opcjonalne i może obejmować część, całość lub żadnego Zlecenia. |
| WRT.19 | Zamawiający w ramach Zlecenia definiuje dowolne bloki tematyczne, o których mowa w wymaganiu WRT.2 dla danej grupy warsztatów. |

# WYMAGANIA W ZAKRESIE DOKUMENTACJI

Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy dokumentację spełniającą wymagania określone w poniższej tabeli.

- minimalne wymagania dla Dokumentacji.

|  |  |
| --- | --- |
| Kod wymagania | Opis funkcjonalności |
| DOK.1 | Zamawiający wymaga, aby Wykonawca przygotował, zgodnie z ogólnie akceptowalnymi standardami w dziedzinie dokumentowania, następujące rodzaje Dokumentacji bezpośrednio związanej z przedmiotem zamówienia: |
| DOK.1.1 | W ramach Projektu Technicznego Wykonawca opracuje i dostarczy następujące dokumenty:   * Plan Wdrożenia Systemu * Plan Testów Akceptacyjnych (PTA), * Szczegółowy opis realizacji wymagań, * Szczegółowy wykaz Oprogramowania (zawierający m.in. producenta, nazwę produktu, wykaz komponentów produktu, typ produktu, typ licencji, ilość licencji, listę polskich dystrybutorów produktu), * Szczegółowy wykaz Urządzeń (zawierający m.in. producenta, nazwę produktu, szczegółowy wykaz podzespołów produktu, kategoria produktu, szczegółowy wykaz licencji produktu, typ licencji, ilość licencji, listę polskich dystrybutorów produktu), * Zapisy licencyjne Oprogramowania Standardowego i Urządzeń, * Opracowanie wysokopoziomowej architektury rozwiązania (zawierający w szczególności model przypadków użycia wraz z ich specyfikacją). * Opracowanie niskopoziomowej architektury rozwiązania * Projekt Infrastruktury Fizycznej Systemu |
| DOK.1.1.1 | Plan Wdrożenia Systemu Kopii Bezpieczeństwa - Wykonawca opracuje i dostarczy dokument zawierający zestaw procedur niezbędnych do instalacji, konfiguracji oraz uruchomienia Urządzeń i Oprogramowania w Lokalizacjach, zarówno do realizacji po stronie Zamawiającego jak i Wykonawcy. Dokument zawierać będzie:   * informacje odnośnie Urządzeń oraz Oprogramowania dla Lokalizacji, w których instalowane będą Urządzenia dla potrzeb dostarczenia Systemu, które są przedmiotem tego zamówienia, * opis czynności wymaganych do realizacji przez Wykonawcę w ramach wdrożenia poszczególnych komponentów Systemu , * harmonogram wdrożenia zależności pomiędzy poszczególnymi krokami i analizę ryzyka oraz procedury powrotu do stanu sprzed uruchomienia. * zestawienie ukazujące przydzielenie poszczególnych licencji do poszczególnych Urządzeń oraz systemów operacyjnych. Dodatkowo Wykonawca musi szczegółowo określić podział licencji m.in. ze względu na jednostki w jakich jest rozliczane dane oprogramowanie tj. ilość procesorów czy PVU (Processor Value Unit), wskazać warunki i czas trwania wsparcia serwisowego producenta. |
| DOK.1.1.2 | Plan Testów Akceptacyjnych (PTA) - dokument PTA musi być przygotowany przez Wykonawcę. |
| DOK.1.1.3 | Szczegółowy opis realizacji wymagań – Wykonawca opracuje dokumentację przedstawiającą szczegółowy sposób spełnienia wszystkich wymagań niniejszego postępowania (w tym wykorzystywanych technologii do spełnienia wymagania). |
| DOK.1.1.4 | Projekt Infrastruktury Fizycznej Systemu – Wykonawca opracuje dokumentację przedstawiającą koncepcję architektury Systemu, w tym w szczególności sposobu realizacji kopii bezpieczeństwa przez Urządzenia i Oprogramowanie oraz ich wykaz. |
| DOK.1.2 | Plan Zarządzania Projektem – dokument musi zawierać zdefiniowane, co  najmniej:   * sposób zarządzania projektem, w tym proces kontroli postępu prac w zakresie kosztów, pracochłonności i zgodności z harmonogramem, a także częstotliwości punktów kontrolnych, raportowanie o postępach w realizacji projektu oraz sposób zarządzania problemami w realizacji projektu, * proces przygotowania planu realizacji przedsięwzięcia w tym planu zapewnienia jakości przedsięwzięcia, * analizę ryzyka przed rozpoczęciem projektu i zarządzanie ryzykiem w trakcie jego realizacji, * sposób zarządzania konfiguracją, w tym identyfikacja elementów konfiguracji, kontrola wersji, informowanie o zmianach, * sposób zarządzania zmianami, w tym rodzaje modyfikacji (poprawki, aktualizacje, rozbudowa, udoskonalenia) oraz procedury kontroli zmian. |
| DOK.1.3 | Dokumentację Powykonawczą, wytworzoną na podstawie dokumentacji powykonawczej dostarczonej przez Zamawiającego po podpisaniu Umowy.  Dokumentacja Powykonawcza będzie zawierać co najmniej następujące informacje:   * Wprowadzenie opisujące cele i zakres przedmiotu zamówienia, * Diagram kontekstowy zaproponowanego rozwiązania i model zachowania, * Ograniczenia rozwiązania, założenia i zależności * Opis wymagań funkcjonalnych i pozafunkcjonalnych Systemu, * Specyfikację wymagań funkcjonalnych i pozafunkcjonalnych, * Specyfikację wymagań Oprogramowania, * Specyfikację wymagań Urządzeń, * Opis i specyfikację interfejsów Urządzeń, * Opis rozwiązania wydajności, skalowalności i niezawodności przebiegu testów akceptacyjnych i sposób oszacowania niezawodności zaproponowanego rozwiązania, w tym propozycję raportów z testów, |
| DOK.1.4 | Dokumentację Eksploatacyjną**,** zawierającą, co najmniej procedury: administracyjne, backupu systemu i danych, awaryjne i użytkownika, przy czym każda z procedur musi zawierać, co najmniej następujące wyszczególnione informacje:   * procedury związane z administracją i eksploatacją, * procedury o charakterze testowym, * procedury działania administratora dla wdrożonego Systemu, * procedury konserwacji wdrożonego Systemu Kopii Bezpieczeństwa, * procedury awaryjne, * procedury kontroli bezpieczeństwa Systemu (Audyt), * procedura identyfikacji i kwalifikacji Błędu, * procedury kwalifikacji zgłoszeń serwisowych, * procedury eskalacji zgłoszeń serwisowych. * Każda z ww. procedur będzie zawierać minimum następujące informacje:   + identyfikator i nazwa procedury,   + rodzaj procedury,   + data utworzenia i zatwierdzenia oraz wersja procedury,   + cel i zakres procedury,   + uzasadnienie zastosowania,   + warunki uruchomienia procedury i oczekiwany oraz możliwy rezultat jej wykonania,   + dane osób, które opracowały procedurę, sprawdziły, zaakceptowały i zatwierdziły,   + wzór formularza zgłoszenia Błędu (dla procedur awaryjnych),   + szczegółowy opis rezultatów,   + możliwe niepowodzenia,   + przebiegi alternatywne,   + algorytm działania, jaki należy zastosować, wykonując kolejne czynności, aby osiągnąć postawiony cel, w tym z informacją o osobie, która powinna wykonać dane czynności. |
| DOK.1.4.1 | Procedury muszą zostać zoptymalizowane pod kątem ciągłości działania usług Systemu Kopii Bezpieczeństwa o wysokim poziomie SLA. |
| DOK.2 | Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak:   * Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób. * Zachowanie standardów, w tym notacji UML, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu. * Zachowanie standardów Zamawiającego w zakresie oznaczeń dokumentów wersjonowania, metryk. * Kompletność dokumentu rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia. * Spójność i niesprzeczność dokumentu rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu. |
| DOK.3 | Cała Dokumentacja, podlega akceptacji Zamawiającego i zostanie dostarczona w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie MS Word i niezabezpieczonym formacie PDF (na płycie CD/DVD lub innym równoważnym nośniku danych) i drukowanej, co najmniej w 1 egzemplarzu (dopuszcza się inne formaty zapisu dokumentacji np. diagramy UML lub formaty wektorowe jak DWG, DXF, należy jednak dołączyć przeglądarkę obsługującą wykorzystane formaty). Diagramy UML sporządzone za pomocą narzędzi CASE muszą być dostarczone w formacie EAP. Dostarczone wykresy Gantta muszą być dostarczone w formacie MPP lub w formacie XLS umożliwiającym import do MS Project. |
| DOK.3.1 | Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu pliki źródłowe zastosowanych w niej obrazów, w tym m.in. schematów, rysunków, topologii oraz wykresów, w formacie niezabezpieczonym i edytowalnym. |
| DOK.3.2 | Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu wszystkie dokumenty robocze wytworzone w takcie realizacji niniejszego zamówienia, w szczególności analizy, arkusze kalkulacyjne, materiały robocze, w formacie elektronicznym, niezabezpieczonym i edytowalnym. |
| DOK.3.3 | Wszystkie Dokumenty przekazane w formie elektronicznej (pliki) muszą:   * być posegregowane w folderach odpowiadających nazwą produktów oraz nazwą, wersją i podwersją przekazywanego modułu (dotyczy kodów źródłowych), * być posegregowane w folderach zgodnie ze strukturą Dokumentacji, * posiadać nazwy plików (razem ze ścieżką) krótsze niż 200 znaków, |
| DOK.3.4 | W przypadku kolejnych wersji Dokumentacji wymagane jest, aby Wykonawca dostarczał elektroniczne wersje Dokumentacji, które zawierają wyróżnione różnice pomiędzy kolejnymi wersjami Dokumentacji (w trybie rejestracji zmian). |
| DOK.4 | Wykonawca w Etapie 3 Umowy dostarczy Zamawiającemu Wykaz Ilościowo-Cenowy przedmiotu zamówienia z podziałem dla każdego Etapu:   1. Urządzenia – wykazanie każdego Urządzenia, wraz ze specyfikacją podzespołów, 2. dokumentów – wykazanie co najmniej Projektu Technicznego, Dokumentacji Powykonawczej, Dokumentacji Eksploatacyjnej, 3. oprogramowania – wykazanie każdego Oprogramowania, 4. usług – wykazanie co najmniej prac instalatorsko-konfiguracyjnych dla Urządzeń oraz Oprogramowania, warsztatów, 5. wartości niematerialne i prawne – wykazanie licencji Oprogramowania i autorskich praw majątkowych do Dokumentacji wytworzonych w Etapie 1, 2, 3.   W zakresie co najmniej:   * + - nazwa,     - producent,     - numer seryjny,     - kod produktu/model,     - opis,     - ilość,     - Lokalizacja instalacji,     - cena jednostkowa brutto w PLN,     - cena jednostkowa netto w PLN,     - wartość brutto w PLN. |
| DOK.5 | Wykonawca przedstawi do akceptacji Zamawiającego dokument ‘Dokumentacja Powdrożeniowa Systemu, zawierający co najmniej:   * Przebieg (wraz ze szczegółowym opisem) prac i czynności wdrożeniowych (w tym napotkanych problemów wraz z opisem ich rozwiązania), * Szczegółowy opis działania wytworzonych w ramach niniejszego Zamówienia procedur (w tym napotkanych problemów jako przebiegi alternatywne wraz z opisem ich rozwiązania), * Szczegółowy opis procedur (wraz z zalecanym harmonogramem) które należy wykonywać w celu prawidłowego utrzymania Systemu, * Raport ze stabilności Systemu z okresu 7 dni od produkcyjnego wdrożenia Systemu. |
| DOK.7 | Wykonawca do Dokumentacji dostarczanej w ramach etapu 1, 2 i 3 dołączy wykaz zawierający szczegółowy spis Dokumentów wraz z opisem ich przeznaczenia. |

# WYMAGANIA W ZAKRESIE OZNAKOWANIA URZĄDZEŃ i DOKUMENTACJI

Minimalne wymagania w zakresie oznakowania Urządzeń i Dokumentacji.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WOZN.1 | Wykonawca zobowiązany jest do:   * Oznakowania dokumentacji, którą wytworzy w ramach realizowanej Umowy; * Oznakowania Urządzeń zakupionych oraz dostarczanych w ramach realizowanej Umowy; * Oznakowania nośników Oprogramowania.   Przez oznakowanie rozumie się: przygotowanie projektu graficznego naklejki do akceptacji Zamawiającego, jej produkcję lub zakup, oraz fizyczne oznakowanie sprzętu i dokumentacji.  Wytyczne dotyczące oznakowania dokumentacji oraz oznaczeń infrastruktury dostarczanej w ramach realizowanej umowy muszą być zgodne z *„Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności 2014 – 2020 w zakresie informacji i promocji”.* |

# WYMAGANIA W ZAKRESIE DOSTĘPNOŚCI

Minimalne wymagania w zakresie dostępności.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| WDSYS.1 | Zapewnienie architektury rozwiązania gwarantującej niezawodność Systemu na  poziomie SLA ustalonym w Umowie, nie mniej niż 99% (niedostępność w skali  miesiąca 7.2 godz.).  SLA liczone jest, jako suma czasu trwania niedostępności Systemu  spowodowanego Błędami Krytycznymi, przy czym okna serwisowe związane  z konserwacją/rekonfiguracją Systemu nie podlegają uwzględnianiu w obliczeniu  SLA (termin i zakres prac realizowanych w ramach okna serwisowego wymaga  uzyskania przez Wykonawcę uprzedniej akceptacji Zamawiającego). |

# WYMAGANIA W ZAKRESIE ZGODNOŚCI Z PRZEPISAMI PRAWA

Minimalne wymagania w zakresie zgodności z przepisami prawa.

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| PR.1 | Rozwiązanie dla Systemu musi być zgodne z niżej wymienionymi aktami prawnym:   * Ustawa o ochronie danych osobowych z dnia 29.08.1997 roku. (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926 z późn. Zm.); * Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12.04.2012 r. (Dz. U. z 2012 r., poz. 526); * Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17.02.2005 roku (tekst jednolity Dz. U. z 2013 r., poz. 235 z późn. zm.); * Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (tekst jednolity Dz. U. z 2009 r. Nr 178, poz. 1380 z późn. zm.); * Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (tekst jednolity Dz. U. z 2014 r., poz. 243); * Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej) - Dz.U.UE.L.2002.108.51 z późn. zm.; |