|  |  |
| --- | --- |
|  | **S**pecyfikacja **I**stotnych **W**arunków **Z**amówienia:  „Dostawa sprzętu komputerowego oraz oprogramowania niezbędnego do realizacji e-Usług wraz z usługą wdrożenia i szkolenia” |

Zatwierdził: ……………………………………………..

Dębica, 10 czerwca 2019 r.

Spis treści

[Wstęp 3](#_Toc2925910)

[Ogólny zarys projektu 3](#_Toc2925911)

[Słownik pojęć 4](#_Toc2925912)

[Wymagania ogólne 6](#_Toc2925913)

[Zakres 1 – Dostawa sprzętu i oprogramowania systemowego 7](#_Toc2925914)

[Serwery 7](#_Toc2925915)

[Macierz dyskowa 9](#_Toc2925916)

[Serwer backupu 12](#_Toc2925917)

[Zasilanie awaryjne – UPS 13](#_Toc2925918)

[Stanowiska robocze stacjonarne 15](#_Toc2925919)

[Infokioski 17](#_Toc2925920)

[Zabezpieczenie e-Usług 20](#_Toc2925921)

[Firewall – UTM – 1 szt. 20](#_Toc2925922)

[Kopie zapasowe 28](#_Toc2925923)

[System zarządzania i monitorowania infrastruktury serwerów 31](#_Toc2925924)

[Licencje 34](#_Toc2925925)

[Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego 36](#_Toc2925926)

[Serwery 36](#_Toc2925927)

[Macierz dyskowa 36](#_Toc2925928)

[Serwer Kopii Zapasowych 36](#_Toc2925929)

[Zasilanie awaryjne – UPS 36](#_Toc2925930)

[Stanowiska robocze 37](#_Toc2925931)

[Zabezpieczenie e-Usług 37](#_Toc2925932)

[Firewall – UTM 37](#_Toc2925933)

[Kopie zapasowe 37](#_Toc2925934)

[Architektura HA dla serwera aplikacji 38](#_Toc2925935)

[Architektura HA dla serwera bazy danych 38](#_Toc2925936)

[Usługi wspomagające 38](#_Toc2925937)

[Zakres 3 – Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym sprzętem i oprogramowaniem 39](#_Toc2925938)

[Zakres 4 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej 41](#_Toc2925939)

[Zakres 5 – Gwarancja i wsparcie 42](#_Toc2925940)

# Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (SzOPZ) w zakresie dostawy i wdrożenia sprzętu oraz oprogramowania służącego uruchomieniu i zabezpieczeniu działania e-Usług w Urzędzie Gminy Miasto Dębica oraz jego jednostkach. Prezentowany poniżej ogólny opis organizacji serwerowni stanowi jedynie zarys całego rozwiązania – Wykonawca może zaproponować swoją wersję organizacji serwerowni o ile proponowane rozwiązanie gwarantowało będzie wyższy poziom bezpieczeństwa i lepsze wykorzystanie mocy obliczeniowej serwerów fizycznych przy czym nie może udostępniać mniejszej szybkości działania. Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne wymagania stawiane oferowanym urządzeniom i oprogramowaniu.

## Ogólny zarys projektu

Celem projektu jest wdrożenie nowoczesnych i bezpiecznych e-Usług w Gminie. W tym celu wszystkie obecne i nowe systemy oraz usługi muszą zostać uruchomione w trybie wysokiej dostępności (HA). Aby sprostać temu wymogowi w Gminie zostaną zainstalowane nowe serwery z usługami wirtualizacji i zabezpieczeniami (niezależnym zasilaniem bateryjnym (UPS) oraz urządzeniem typu UTM). Wszystkie nowe i obecne usługi zostaną uruchomione w środowisku wirtualnym w trybie HA.

Fizycznym miejscem instalacji e-Usług będzie lokalizacja główna.

Aby usługi elektroniczne świadczone były w sposób bezpieczny, serwerownia zostanie wyposażona w urządzenie typu UTM zabezpieczające ruch sieciowy pomiędzy petentami i placówką oraz gwarantującymi ciągłość dostępności e-Usług.

Niniejszy Przedmiot Zamówienia podzielony jest na następujące zakresy:

|  |  |  |
| --- | --- | --- |
| Lp. | Opis prac wykonanych w ramach zakresu | Maksymalny czas realizacji |
| Zakres 1 | Dostawa sprzętu i oprogramowania systemowego. | 45 dni[[1]](#footnote-1) |
| Zakres 2 | Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego. | 10 dni[[2]](#footnote-2) |
| Zakres 3 | Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym sprzętem. | 14 dni2 |
| Zakres 4 | Przygotowanie oraz dostarczenie dokumentacji projektowej i powykonawczej. | 14 dni2 |
| Zakres 5 | Świadczenie usług gwarancji i rękojmi w ramach całości dostarczonego rozwiązania (zgodnie z ofertą) | Min. 36 miesięcy[[3]](#footnote-3) - zgodnie z ofertą |

## Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

1. **Dysfunkcja** – zbiorcze określenie dla nieprawidłowości rozumianych jako niezgodność z Dokumentacją lub też uciążliwość w pracy z Systemem.
2. **Kategoria Dysfunkcji** - kategoria, do której kwalifikowane jest Zgłoszenie Serwisowe dotyczące Dysfunkcji. Opisane szczegółowo w Załączniku nr 6 do Umowy.
3. **Prace Serwisowe** - działania Wykonawcy mające na celu realizację Zgłoszenia Serwisowego.
4. **Naprawa** – modyfikacja Systemu usuwająca Dysfunkcję Systemu.
5. **Obejście** - tymczasowe rozwiązanie pozwalające na prawidłowe wykorzystanie oprogramowania bez usuwania wykrytego błędu przy zachowaniu integralności bazy danych.
6. **Realizacja Zgłoszenia Serwisowego** - zakończenie Prac Serwisowych, w wyniku których przywrócono Stan Funkcjonalności.
7. **Analiza** – dokumenty opracowane przez Wykonawcę, mające na celu doprecyzowanie sposobu realizacji wymagań Zamawiającego, zasad i metod realizacji Umowy oraz wskazanie i szczegółowe opisanie Produktów;
8. **Backup** – wykonanie kopii bezpieczeństwa danych pozwalających na odtworzenie i przywrócenie Bazy Danych i Systemu po wystąpieniu awarii w przypadku utraty lub uszkodzenia oryginalnych danych; jakość odtworzonych danych powinna być dostosowana do ustalonego uprzednio poziomu ryzyka, który poniesie Zamawiający (poziom ryzyka determinuje cykliczność wykonywania backup’ów).
9. **Baza Danych** – zbiór wszystkich danych zewidencjonowanych za pomocą Systemu.
10. **Czas Roboczy** – czas pracy liczony w Dni Robocze, w którym świadczona jest pomoc telefoniczna przy eksploatacji Systemu.
11. **Dzień Roboczy** – dzień kalendarzowy od poniedziałku do piątku z wyłączeniem świąt i dni ustawowo wolnych od pracy.
12. **Dokumentacja** – dokument papierowy lub elektroniczny opisujący System i zasady użytkowania Systemu. Wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy.
13. **Godziny robocze** – czas pracy liczony w Dni Robocze w godzinach 7:30 – 15:30.
14. **Konsultant** – osoba fizyczna posiadająca odpowiednie kwalifikacje uprawniające do realizowania Serwisu.
15. **Pomoc Telefoniczna** – świadczenie konsultacji telefonicznej dotyczące szeroko pojętej eksploatacji Systemu.
16. **Procedura** – schemat postępowania w jaki winien być realizowany określony fragment Przedmiotu Umowy.
17. **Publikacja** – udostępnienie Systemu zawierającego zmienioną funkcjonalność.
18. **Serwer** – sprzęt komputerowy, na którym zainstalowana jest baza danych lub aplikacje wykorzystywane przez System.
19. **Serwis** – usługa o charakterze technicznym, organizacyjnym, doradczym i szkoleniowym, przeznaczona do zapewnienia stabilnej pracy Systemu.
20. **Stan Funkcjonalności** - stan Systemu, w którym nie występują Dysfunkcje.
21. **Upgrade** – nowa  wersja Systemu związana ze stworzeniem nowej funkcjonalności.
22. **Update** – aktualizacja Systemu w wyniku zmian przepisów, związanych bezpośrednio i pośrednio z systemem ochrony zdrowia, w zakresie tej samej wersji Systemu.
23. **Wdrożenie** – opisane Umową świadczenia Wykonawcy mające na celu uruchomienie systemu serwerów wirtualnych w trybie HA.
24. **Wersja** – okresowa Publikacja Systemu uwzględniająca Naprawy i zmiany dokonane w okresie od poprzedniej Publikacji Systemu. Wydanie Wersji obejmuje również opis nowej Funkcjonalności Systemu.
25. **Zgłoszenie Serwisowe** – Dysfunkcja, o której Wykonawca został powiadomiony drogą mailową.
26. **Administrator** - Użytkownik konfigurujący i zarządzający Systemem i Infrastrukturą.
27. **Architektura systemu teleinformatycznego** – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami.
28. **Czas dostarczenia rozwiązania** - Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Rozwiązania Zastępczego.
29. **Dostępność** – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym .
30. **Integralność** – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony .
31. **Moduł systemu** – kompletny zestaw narzędzi informatycznych obejmujących wszystkie warstwy architektury systemu, który dostarcza aplikację przeznaczoną dla użytkownika końcowego do realizacji określonych dziedzin działalności Zamawiającego.
32. **Oprogramowanie standardowe** – Każde oprogramowanie niezbędne do działania Systemu.
33. **PKI** – Infrastruktura Klucza Publicznego
34. **Rozwiązanie zastępcze** - proponowane przez Wykonawcę rozwiązanie tymczasowe, usuwające lub niwelujące czasowo do akceptowalnego poziomu skutki wystąpienia Wady, wprowadzone do czasu usunięcia Wady.
35. **System** – Łączne określenie dla oprogramowania i sprzętu – występującego u Zamawiającego, objętego wdrożeniem oraz umową serwisową z Wykonawcą, bez względu na nazwę handlową. Obejmujący platformę systemowo-sprzętową, oprogramowania aplikacyjne oraz inne oprogramowanie niezbędne do działania e-Usług realizowanych w niniejszym zamówieniu dostarczanych przez Wykonawcę.
36. **System zewnętrzny** - Każdy System informatyczny niebędący przedmiotem Zamówienia a oddziaływujący na przedmiot zamówienia.
37. **Użytkownik** - Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło.
38. **Wykonawca** – wybrany w drodze zamówienia publicznego podmiot realizujący niniejszy przedmiot zamówienia.
39. **Zamawiający** – Gmina Miasto Dębica
40. **Zdalny dostęp** – możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.
41. **ASI** – Administrator Systemów Informatycznych u Zamawiającego

# Wymagania ogólne

Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).

System musi być zbudowany w architekturze wysokiej dostępności (HA).

System musi umożliwiać definiowanie dowolnej ilości użytkowników.

System musi posiadać graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po dowolnych kryteriach. Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, itp. dla których wymogi minimalne co do posiadanych interfejsów zostały opisane odrębnie.

System musi gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych.

System musi pracować w środowisku sieciowym i posiadać wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników bez ograniczeń na ich liczbę.

System musi posiadać mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych.

System musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji.

Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne okresowe [np. na aktualizację systemu zabezpieczeń] na min. okres zaoferowanej gwarancji na urządzenie na którym licencje są instalowane; nośniki instalacyjne, instrukcje.

Zamawiający dokona odbioru przedmiotu Umowy dwuetapowo, zgodnie z załącznikami nr 9.1 oraz 9.2 do SIWZ.

**Minimalny okres gwarancji - 36 msc. - dotyczy wszystkich elementów systemu – o ile w specyfikacji i/lub ofercie nie wyszczególniono inaczej (np. baterie UPS).**

# Zakres 1 – Dostawa sprzętu i oprogramowania systemowego

Poniżej przedstawiono parametry minimalne jaki dostarczany sprzęt musi spełniać. W przypadku gdy do realizacji Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nie ujęte w poniższym zestawieniu Wykonawca musi go dostarczyć i wykazać w wykazie asortymentowo-cenowym.

## Serwery

Serwery aplikacyjne – min. 2 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Obudowa | RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia), maksymalnie 2U |
| Procesor | Dwa procesory. Płyta główna wspierająca zastosowanie procesorów min. do 28 rdzeniowych. |
| Min. 8-rdzeniowe[[4]](#footnote-4) klasy x86 - 64 bity, osiągające w testach w testach PassMark – dual CPU Mark wynik nie gorszy niż 16800 punktów. wynik testu musi być opublikowany na stronie cpubenchmark.net |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania min. 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5”  System wirtualizacji zainstalowany na nośnikach pracujących w trybie RAID-1, bez konieczności użycia dysków twardych. Wykonawca musi dostarczyć nośniki danych (min. 8GB każdy). Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. |
| Kontroler | Serwer wyposażony w 2-portowy kontroler sprzętowy SAS typu external, obsługujący poziomy: RAID 0/1/10/5 |
| Pamięć operacyjna | min. 128 GB DIMM DDR4 w modułach o pojemności min. 16GB każdy. |
| Sloty rozszerzeń | 2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16 |
| Interfejsy sieciowe | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.  Minimum 2 porty 10Gb/s (SFP+ wraz z zainstalowanymi wkładkami). |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | Min.: 4 x USB (co najmniej jeden z przodu obudowy); 1x VGA; |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy min. 500W. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug.  Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia do 45°C, zgodność ze standardem ASHRAE Class A4 |
| Karta/moduł  zarządzający | Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, posiadająca minimalną funkcjonalność:  • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe  • wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP  • dostęp do karty zarządzającej poprzez  − dedykowany port RJ45  − przez współdzielony port zintegrowanej karty sieciowej serwera  • dostęp do karty możliwy  − z poziomu przeglądarki webowej (GUI)  − z poziomu linii komend  − poprzez interfejs IPMI 2.0  • wbudowane narzędzia diagnostyczne  • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego  • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników  • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)  • obsługa zdalnego serwera logowania (remote syslog)  • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów  • funkcja zdalnej konsoli szeregowej - przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności  • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji  • zdalna aktualizacja oprogramowania (firmware)  • możliwość równoczesnej obsługi przez min. 2 administratorów  • wsparcie dla Microsoft Active Directory  • obsługa SSL i SSH  • enkrypcja AES/3DES dla zdalnej konsoli  • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3  • wsparcie dla Integrated Remote Console for Windows clients  • możliwość autokonfiguracji sieci karty zarządzającej (DHCP)  Rozwiązanie sprzętowe posiadające dedykowany port RJ45. |
| Wsparcie dla systemów operacyjnych i wirtualizacyjnych | Min.: Microsoft Windows Server 2016, Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server, VMware ESXi 6.5 i nowsze |
| Gwarancja | Z czasem naprawy NBD. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie, potwierdzające pochodzenie oferowanego urządzenia z oficjalnego kanału dystrybucyjnego producenta. |

## Macierz dyskowa

Macierz dyskowa przechowywująca dyski maszyn wirtualnych i dane użytkowników – 1 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U. |
| Przestrzeń dyskowa | Macierz musi udostępniać minimum 16 TB przestrzeni RAW zbudowanej w oparciu o minimum 11 dysków w technologii SAS o prędkości obrotowej min. 10k obr/min; min. 1,6 TB przestrzeni RAW zbudowanej w oparciu o min. 2 dyski SSD. |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 100 dysków twardych. |
| Obsługa dysków | Macierz musi obsługiwać dyski SSD, SAS i NLSAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NLSAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5 oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych.  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Oferowana konfiguracja dyskowa musi zawierać min. rekomendowaną przez producenta ilość dysków spare. |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe poprzez interfejsy SAS. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | Każdy kontroler macierzowy musi być wyposażony w minimum 6 GB pamięci cache. Powyższa pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM – nie zezwala się użycia dysków SSD. Pamięć zapisu musi być mirrorowana pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 12 miesięcy.  Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD. |
| Interfejsy | Macierz musi posiadać, co najmniej 4 aktywne porty SAS 12 Gb/s. |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i konsoli CLI. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 200 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Kopie pełne i migawkowe | Macierz musi umożliwiać dokonywania na żądanie min. 200 tzw. migawkowych kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą relokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Zdalna replikacja danych | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem. |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, Vmware. Macierz musi posiadać wsparcie dla różnych systemów klastrowych, co najmniej Microsoft Cluster. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek – jeśli wymagane. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych lub wielu serwerów. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Wraz z macierzą mają zostać dołączone kable SAS umożliwiające podłączenie serwerów - w ilości min. 8 szt. |
| Gwarancja | Gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez 24 godziny na dobę. Czas naprawy NBD.  W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. |

## Serwer backupu

Serwer wykonywania i przechowywania kopii bezpieczeństwa – 1 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor | Dedykowany do obsługi urządzeń typu NAS z obsługą instrukcji x86 i aktywną funkcją wirtualizacji |
| Obudowa | Rack, max. 2U, szyny montażowe w zestawie |
| Pamięć RAM | min. 16 GB RAM |
| Interfejsy sieciowe | Min: 4 x Gigabit (10/100/1000) |
| Dyski | Zatoki na min. 8 dysków SATA III  Zainstalowane min. 6 dysków SATAIII:  o pojemności min. 10TB każdy,   * pamięć podręczna: min. 128MB, * prędkość obrotowa: min. 7200RPM, * MTBF: min. 2 000 000 h, * maks. wew. szybkość przesyłania: min. 200 MB/s. |
| Porty | Min. 1x USB 3.0 |
| Wskaźniki LED | Min. status HDD, Power |
| Obsługa RAID | Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk. |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Wspierane systemy operacyjne | Microsoft Windows Server 2016, Linux, Vmware |
| Protokoły | CIFS, AFP, NFS, FTP, iSCSI, Telnet, SSH, SNMP |
| Wirtualizacja | Certyfikat zgodności Vmware Ready, Windows Server 2016 Certified. możliwość uruchomienia maszyn wirtualnych bezpośrednio na serwerze backupu bez konieczność posiadania zewnętrznych wirtualizatorów. |
| Szyfrowanie | Szyfrowanie ze wsparciem sprzętowym całych woluminów oraz wybranych udziałów sieciowych |
| iSCSI | Wbudowany inicjator i target iSCSI |
| Replikacja | Replikacja między urządzeniami w czasie rzeczywistym |
| Kontroler domeny | Możliwość podłączenia do kontrolera domeny Microsoft |
| Liczba iSCSI LUN | Min. 64 |
| Liczba kont użytkowników | Min. 200 |
| Liczba grup | Min. 100 |
| Liczba udziałów | Min. 100 |
| Liczba jednoczesnych połączeń | Min. 500 |
| Zasilanie | Redundantne 2x max. 450W |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |

## Zasilanie awaryjne – UPS

Zasilacz UPS do serwerowni -1 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc znamionowa | Min. 3000VA |
| Topologia | Line-interactive |
| Obudowa | Do montażu w szafie Rack 19” |
| Maksymalna wysokość UPS | Maks. 3U |
| Maksymalna głębokość | Maks. 700 mm |
| Zakres napięcia wejściowego | 190–260 V |
| Napięcie nominalne wyjściowe | 220/230/240 V |
| Gniazda wyjściowe | Min. 8 szt. (10A) |
| Sprawność | Min. 90% |
| Częstotliwość wyjściowa | 50/60 Hz +/- 0,1% (autodetekcja) |
| Czas podtrzymania dla obciążenia 100% | Min. 20 minut |
| Czas podtrzymania dla odciążenia 50% | Min. 40 minut |
| Obsługa dodatkowych baterii | do 4 modułów bateryjnych o wysokości max 2U każdy |
| Zarządzanie akumulatorami | System ładowania nieciągłego baterii z kompensacją temperatury, automatyczne sprawdzanie akumulatorów, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie dodatkowych zewnętrznych modułów bateryjnych, wymiana akumulatorów „na gorąco” bez konieczności wyłączania podłączonych urządzeń. |
| Interfejs użytkownika | Wyświetlacz LCD (informacje o statusie i pomiarach UPS, możliwość pomiaru zużycia energii w kWh) |
| Standardowe gniazda komunikacyjne | Karta sieciowa + 1 x styki przekaźnikowe + 1 mini złącze zdalnego zał./wył. i wyłączenia |
| Zdalne zarządzanie | * Kompatybilność z HTTP, SNMP, SMTP, Telnet, SSL, SSH * Zdalne sterowanie i ponowne uruchamianie urządzeń chronionych przez UPS, poprzez sieć SNMP/Web, * Konfigurowalne akcje zawierające automatyczne zamykanie systemów w przypadku przedłużających się przerw w zasilaniu * Powiadamianie e-mailowe o alarmach * Kompatybilność z SNMPv3 i IPv6 * Konfigurowalne automatycznie powiadamiania e-mail w odpowiedzi na alarmy UPS oraz przesyłanie raportów okresowych * Sterowanie załączaniem i wyłączaniem UPS poprzez przeglądarkę internetową * Ustawianie i sterowanie segmentami odbiorników poprzez interfejs przeglądarki internetowej, z sekwencyjnym załączaniem i optymalizacją czasu podtrzymania bateryjnego poprzez wcześniejsze zamykanie systemów o mniejszym znaczeniu. * Pomiar wilgotności i temperatury z opcjonalnym czujnikiem monitorowania środowiska * Automatyczne ustawienia daty i godziny poprzez serwer NTP * Zabezpieczenie hasłem * Transmisja SSL * Zapis dziennika zdarzeń w pamięci trwałej |
| Temperatura pracy | Min. od 10°C do 40°C |
| Bezpieczeństwo, zakłócenia elektromagnetyczne | IEC/EN 62040-1-1, IEC/EN 62040-2 |
| Certyfikaty | CE, raport CB, TÜV |
| Gwarancja na akumulatory | Min. 2 lata |
| Oprogramowanie do zarządzania i monitoringu UPS | Pakiet oprogramowania kompatybilny z MS Windows Server oraz RedHat Linux, włącznie z oprogramowaniem wirtualizacyjnym, takim jak Vmware i Hyper-V. Oprogramowanie z aktywną funkcją wyłączania systemu w przypadku długotrwałej przerwy w dostawie energii. Możliwa rozbudowa licencji o funkcje: zawieszania działania niekrytycznych maszyn wirtualnych, konsolidowania krytycznych maszyn wirtualnych, wyłączania nieużywanych serwerów i wydłużania przez to czasu pracy z akumulatora, przenoszenia maszyny wirtualnej lub łagodnego wyłączania systemu. |
| Wyposażenie dodatkowe | Zestaw gniazd wyjściowych PDU o prądzie nominalnym 16A podłączany do gniazda wyjściowego w zasilaczu awaryjnym UPS, obudowa 1U do montażu w szafie Rack (19”) z możliwością montażu w wielu położeniach z 12 szt. gniazd IEC-320-C13 (10A) i 1 szt. IEC-320-C19 (16A) (z 2 bezpiecznikami nadprądowymi), z zaciskami zabezpieczającymi przed przypadkowym wyciagnięciem kabla zasilającego na gniazdkach wejściowych i wyjściowych. Czujnik monitorowania środowiska UPS umożliwiający zdalne monitorowanie temperatury, wilgotności i dwóch urządzeń stykowych podłączany do karty sieciowej SNMP. |

## Stanowiska robocze stacjonarne

Komputer – 87 szt.:

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Procesor/Chipset | Wielordzeniowy, min. 8000 pkt. w teście PassMark - CPU Mark |
| Karta graficzna | min. 400 pkt. w teście PassMark - G3D Mark |
| System operacyjny | Umożliwiający uruchomienie systemów dziedzinowych Zamawiającego bez użycia wirtualizacji w wersji pozwalającej na zarządzanie systemem za pomocą domeny Active Directory. |
| Oprogramowanie biurowe | Oprogramowanie biurowe zawierające, min: arkusz kalkulacyjny, edytor tekstu, program do tworzenia prezentacji. Zainstalowane oprogramowanie biurowe w wersji licencjonowania przeznaczonej dla Zamawiającego (możliwe zastosowanie oprogramowania OpenSource) oferujące w 100% zgodność z posiadanym przez Zamawiającego oprogramowaniem MS Office w wersjach 2007 – 2016 w zakresie dokumentów tekstowych, arkuszy kalkulacyjnych i prezentacji. Oferowane oprogramowanie musi wiernie odwzorowywać wszystkie elementy (1:1) każdego dokumentu utworzonego w dowolnej posiadanej wersji MS Office, zwłaszcza w zakresie formatowania nagłówków, stopek, numerowania, układów tabel, formatowania obrazów i grafiki typu „wordart”. Oferowane oprogramowanie musi umożliwiać automatyzację korespondencji w oparciu o różne listy (np. CSV, XLS, TXT, czy źródła ODBC). Oprogramowanie musi wspierać wszystkie funkcje i narzędzia MS Excel (np. tabele i wykresy przestawne). Oprogramowanie musi wspierać wszystkie animacje dostępne w MS Powerpoint 2016. Oprogramowanie musi posiadać możliwość automatyczego aktualizaowania i instalowania poprawek bez potrzeby zakupu odrębnego oprogramowania (np. z poziomu narzędzia Update Microsoftu). |
| Pamięć masowa | Min. 240GB SSD, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.  Dodatkowy dysk (dopuszczalny talerzowy) o pojemności min. 500GB. |
| Napęd optyczny | min. DVD-RW |
| Pamięć RAM | min. 8GB |
| Sieć | 10/100/1000 Ethernet |
| Porty wbudowane | min. 6 USB (w tym co najmniej 2 porty 3.0), 1 RJ45, 1 VGA (DisplayPort lub D-SUB lub HDMI) – zgodny z zaoferowanym monitorem, audio jack, ethernet. |
| Akcesoria w zestawie | Klawiatura i mysz przewodowe. |
| Moc pobierana | <250W średnio |
| Zasilanie: | 220-240V @ 50Hz |
| Wymiary max. obudowy komputera (szer. x głęb. x wys) | 100mm x 300mm x 300mm |
| Waga komputera | max. 6kg |
| Temperatura pracy | min. 10° do 40° C |
| Certyfikaty | TÜV-GS, EN 60950 RF Interference: FCC Class B, Ergonomics CE, VCCI, RoHS Compliant |
| Warunki gwarancji | Dyski podlegające wymianie zostają u Zamawiającego. |
| UWAGA | Wraz z zestawami należy dostarczyć:   * Kabel zasilający, * klawiaturę i mysz optyczną – przewodowe.   Oferowana seria komputera musi posiadać certyfikat potwierdzający poprawną współpracę oferowanego komputera z zaoferowanym systemem operacyjnym. |

Monitor – 87 szt.:

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Ekran | min. 23,5 cala, Full HD 1920 x 1080 @ 60 Hz, proporcje: 16:9, Powłoka antyodblaskowa/matowa |
| Jasność | min. 240 cd/m2 |
| Kontrast | min. 1000:1 (statyczny) |
| Złącza | min. 1 złącze cyfrowe (DP lub HDMI lub DVI) |
| Podstawka | z możliwością pochylenia o min. +10° |
| Waga monitora | max. 5kg |
| Zasilanie | Max 35W, z sieci 240VAC |
| UWAGA | Wraz z zestawami należy dostarczyć:   * kabel odpowiedni do podłączenia monitora z komputerem, * kabel zasilający, |

## Infokioski

Zamawiający wymaga dostarczenia 2 szt. kiosków spełniających następujące wymagania techniczne i funkcjonalne:

1. Przyjmowanie wpłat i opłat z tytułów zdefiniowanych przez Zamawiającego

2. Przyjmowanie płatności w postaci bezgotówkowej za pomocą:

a) stykowych kart płatniczych systemów Visa i MasterCard,

b) bezstykowych kart płatniczych systemów Visa PayWave i Mastercard PayPass,

c) możliwość potwierdzenia transakcji przy pomocy zabudowanej klawiatury do wprowadzenia nr PIN

d) płatność za pomocą systemów NFC;

3. Musi umożliwiać identyfikację tytułu opłaty oraz danych wpłacającego:

a) poprzez wybór pozycji z menu i uzupełnienie dodatkowych niezbędnych danych,

b) poprzez ręczne wprowadzenie niezbędnych danych do identyfikacji;

c) poprzez automatyczny odczyt danych przy wykorzystaniu skanera dowodu osobistego;

d) poprzez odczytanie kodu jedno lub dwuwymiarowego z blankietu wpłaty;

4. Musi umożliwiać wprowadzenie danych o realizowanej usłudze poprzez wybór z poniższych opcji:

a) automatyczny odczyt danych przy wykorzystaniu czytnika kodów jedno- oraz dwuwymiarowych;

b) ręczny wybór usługi z katalogu zdefiniowanych usług do realizacji w danym info kiosku;

c) wprowadzenie danych z poziomu klawiatury pełnowymiarowej z touchpadem,

5. Musi mieć możliwość przerwania realizacji transakcji w każdym momencie;

6. Musi umożliwiać blokowanie możliwości sprzedaży w przypadku braku papieru w drukarce lub niesprawności technicznej info kiosku;

7. Musi posiadać funkcjonalność drukowania potwierdzenia anulowania transakcji kartą płatniczą.

8. Musi umożliwiać wydruk potwierdzenia udanej/nieudanej operacji płatności kartą płatniczą,

9. Musi mieć możliwość wydruku potwierdzenia dokonania wpłaty/opłaty,

10. Obsługa dedykowanej aplikacji infokiosku musi być realizowana za pomocą wielofunkcyjnego ekranu dotykowego, dostępne funkcje muszą być wyświetlane za pomocą zintegrowanego wyświetlacza LCD;

11. Musi umożliwiać generowanie odpowiednich sygnałów graficznych potwierdzających, negujących, ostrzegających - w związku z wykonywanymi operacjami;

12. Oprogramowanie musi pracować w przynajmniej w dwóch trybach: informacyjno-płatniczym oraz serwisowym;

13. W trybie informacyjno-płatniczym funkcje serwisowe nie są dostępne dla klienta;

14. W trybie serwisowym istnieje możliwość konfiguracji urządzeń peryferyjnych, weryfikacji statusu urządzeń, podglądu zdarzeń,

15. Musi realizować rejestrację, na lokalnym nośniku danych, wszystkich zdarzeń,

16. Musi posiadać moduł transmisji danych odpowiedzialnych za transmitowanie na bieżąco żądań obsługi serwisowej: awarie urządzeń, sygnalizację końca zapasu papieru, otwarcie obudowy oraz pozostałe, niezbędne do pracy sygnały,

17. Obudowa musi być wykonana ze stali pomalowanej proszkowo na kolor z palety RAL ustalony z Zamawiającym,

18. Infokiosk musi być mocowany na stałe do podłoża w sposób uniemożliwiający jego kradzież,

19. Krawędzie zewnętrzne i wewnętrzne muszą być ukształtowane tak, aby nie spowodowały uszkodzeń odzieży lub zranienia użytkownika (interesant, serwisant, etc.),

20. Gabaryty urządzenia nie przekraczają wymiarów: 1600 x 1400 x 650 mm (wys. x szer. x gł.),

21. Dostęp do wnętrza obudowy musi być zabezpieczony zamkiem patentowym,

22. Na obudowie muszą być umieszczone informacje dotyczące obsługi infokiosku, w sposób uzgodniony z Zamawiającym, jak również inne elementy graficzne (charakterystyczne dla Zamawiającego),

23. Infokiosk musi być wyposażony w ekran dotykowy zapewniający wygodne korzystanie z funkcji infokiosku przez użytkownika.

24. Musi mieć możliwość obsługiwania dłonią, dłonią osłoniętą rękawiczką, lub przedmiotem – np. ołówek itp.

25. Minimalne wymagania dla ekranu LCD i ekranu dotykowego głównego:

a) kolorowy wyświetlacz graficzny o przekątnej 19”,

b) jasność ekranu minimum 300 cd/m2,

d) w przypadku braku aktywności (interakcji z pasażerem) na ekranie startowym przez zadany czas, wyświetlacz musi przechodzić do ekranu startowego.

26. Infokiosk musi być wyposażony w zestaw do płatności kartowych (terminal płatniczy) z użyciem kart organizacji płatniczych, w wersji tzw. unattended , tzn. do samodzielnej obsługi przez użytkownika, o podwyższonej odporności, składający się z:

a) czytnika zbliżeniowych kart płatniczych wraz z dedykowaną aplikacją płatniczą, umożliwiający transakcje kartami płatniczymi, przynajmniej w standardzie Visa i Mastercard; rozwiązanie posiada certyfikaty:

• EMV Contactless Level 1, MasterCard PayPass M/Chip, Visa qVSDC,

• qVSDC (Visa Europe) oraz TIP Contactless (MasterCard International) - dla aplikacji płatniczej do współpracy z agentem rozliczeniowym Zamawiającego.

b) czytnika stykowych kart płatniczych wraz z dedykowaną aplikacją płatniczą, umożliwiający transakcje kartami płatniczymi, przynajmniej w standardzie Visa i Mastercard; rozwiązanie posiada certyfikaty:

• EMV Level 1 i Level 2,

• ADVT (Visa Europe) oraz TIP (MasterCard International) - dla aplikacji płatniczej do współpracy z agentem rozliczeniowym,

c) PIN-pad służący do autoryzacji transakcji kodem PIN; klawisze PIN-pada wykonane muszą być ze stali nierdzewnej.

27. Infiokiosk musi być zasilany z zewnętrznego źródła zasilania z sieci 230V, 50Hz,

28. Pobór mocy nie może być wyższy niż 350W w standardowym trybie pracy,

29. Odbiornik prądu w Infokiosku musi posiadać własny obwód z oddzielnym zabezpieczeniem (bezpiecznikiem) i układem różnicowoprądowym,

30. Infokiosk musi być wyposażony we własny akumulator, podtrzymujący pracę urządzenia w przypadku zaniku napięcia zasilającego, co najmniej na czas umożliwiający kontrolowane zamknięcie systemu,

31. Akumulator musi posiadać automatyczny układ ładujący w oparciu o zasilanie zewnętrzne o parametrach dostosowanych do jego charakterystyki,

33. Infiokiosk musu być wyposażony w moduł transmisji danych w oparciu o sieć bezprzewodową spełniającą parametry minimum GSM/GPRS/UMTS lub o złącze Ethernet,

34. Moduł transmisji danych musi mieć możliwość przesyłania danych konfiguracyjnych i aktualizacji z systemu centralnego.

## Zabezpieczenie e-Usług

### Firewall – UTM – 1 szt.

Platforma służąca zabezpieczeniu dostępu do systemu EZD oraz do innych usług zainstalowanych u Zamawiającego, pozwalająca na filtrowanie ruchu z/do internetu do/z sieci LAN. Platforma musi umożliwiać kontrolę w warstwie aplikacji oraz umożliwiać zdalny dostęp do sieci LAN zamawiającego jednostkom zewnętrznym. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Typ systemu ochrony** | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, o zalecanej przez producenta mocy obliczeniowej wystarczającej do zabezpieczenia około 200 komputerów w sieci LAN oraz minimum 6 aplikacji webowych zainstalowanych w infrastrukturze Zamawiającego w trybie HA z obsługą loadbalancingu.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy. |
| **Wymagania systemowe** | Obsługa nielimitowanej ilości hostów w sieci chronionej.  Typ procesora: multi-core  Pamięć RAM: nie mniej niż 6 GB  Obudowa przeznaczona do montażu w szafie RACK.  Minimalna liczba i typ interfejsów fizycznych: 6x GE (IEEE 1000Base-T), USB (Type-A), 1x Console (RJ-45 lub DB9)  Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)  Minimalna liczba nowych połączeń na sekundę: 100000  Minimalna liczba jednoczesnych połączeń: 7000000  Minimalna przepustowość Firewall: 6000 Mbps  Minimalna przepustowość IPS: 4000 Mbps  Minimalna przepustowość Web Proxy AV: 2000 Mbps  Minimalna przepustowość IPSec: 100 Mbps  Minimalna liczba równoczesnych tuneli IPSec VPN: 1000  Minimalna liczba równoczesnych tuneli SSL VPN: 100  Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB. |
| **Zarządzanie i utrzymanie** | Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).  Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup.  Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.  Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.  Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.  System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.  System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.  Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).  System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.  Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora (np. zmiana zapomnianego hasła).  System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.  Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.  System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.  Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpowiednik).  System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych, itp.). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do min. 12 miesięcy w ramach webowego interfejsu graficznego urządzenia.  System powinien oferować możliwość integracji z centralnym systemem do zarządzania.  Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego lub do serwera FTP.  Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: np. codziennie, raz w tygodniu lub raz w miesiącu.  Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.  Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.  Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.  Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).  System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.  W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie). |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | Wymagane jest aby zapora sieciowa mogła działać w oparciu o mechanizm Stateful Deep Packet Inspection.  Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa.  System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.  Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.  Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.  System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL, VPN.  Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.  Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.  System powinien zapewniać ochronę przed:   * atakami DoS czy DDoS (flood protection). * skanowaniem portów (portscan blocking).   System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).  Rozwiązanie powinno zapewniać obsługę:   * routingu statycznego. * protokołów routingu dynamicznego. * Protocol Independent Multicast Sparse Mode (PIM-SM). * IGMP snooping. * przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy). * serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. * usług DNS, DHCP oraz NTP. * IEEE 802.3Q VLAN z niezależnymi pulami DHCP. * Policy Based Routing oraz Multipath Rules. * agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). * IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6.   Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP.  Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).  Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.  Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.  Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta. |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.  Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.  System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. |
| **Autoryzacja użytkowników** | Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 300 kont.  System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.  Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.  Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal. |
| **Samoobsługowy portal dla użytkowników** | Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci – jeśli wymagany.  Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).  Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.  Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika. |
| **Opcje VPN** | System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:  Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)  Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu portalu użytkownika). |
| **IPS** | Dodatkowy moduł ochrony klasy IPS z bazą sygnatur dostarczoną i uaktualnianą przez producenta.  Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.  Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.  System powinien generować alerty w przypadku wykrycia ataku. |
| **ATP** | System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami. |
| **Sprzętowy VPN** | System ochrony powinien posiadać możliwość centralnego zdalnego zarządzania sprzętowymi klientami VPN, pochodzącymi od tego samego producenta. |
| **WWW VPN** | Udostępnianie zasobów w sieci LAN w postaci usług http/HTTPS, RDP, VNC, SSH, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5. |
| **Ochrona i kontrola Web** | Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.  Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).  System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.  System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.  Rozwiązanie powinno automatyczne odpytywać bazy producenta w trybie rzeczywistym.  Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym lub partiami.  Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.  System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.  System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.  Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów, cookies.  System powinien zapewniać możliwość emulacji skryptów JavaScript.  Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem „SafeSearch” (min. google).  Rozwiązanie powinno zawierać zdefiniowane przez producenta kategorie stron www i umożliwiać tworzenie własnych kategorie.  Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać blokadę stron HTTPS.  Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dla użytkowników i grup użytkowników.  System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo urzędu. |
| **Ochrona i kontrola aplikacji EZD oraz Portalu e-Usług** | Rozwiązanie powinno oferować bazę danych producenta opisującą aplikacje sieciowe.  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.  Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.  Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania (na podstawie analizy ruchu).  Rozwiązanie powinno umożliwiać blokowanie:  - aplikacji, które pozwalają na transfer plików (np. P2P).  - komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.  - proxy uruchamianych poprzez przeglądarki internetowe.  - streaming media (radio internetowe, Youtube, Vimeo).  Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo. |
| **Kształtowanie pasma dla Web i Aplikacji Portalu e-Usług** | Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie.  Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.  Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared). |
| **Ochrona i kontrola Email** | Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Mail Transfer Agent.  System powinien umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS.  Rozwiązanie powinno zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur zagrożeń.  System powinien zapewniać wykrywanie, blokowanie i skanowanie załączników.  Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar.  System powinien wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości.  Rozwiązanie powinno oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora (np. numer PESEL).  System powinien oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP oraz IMAP.  Rozwiązanie powinno umożliwiać archiwizowanie wiadomości email.  Rozwiązanie powinno współpracować z bazami RBL.  Rozwiązanie powinno umożliwiać tworzenie białych i czarnych list adresów IP i email.  Rozwiązanie powinno zapewniać wykrywanie spamu niezależnie od stosowanego języka.  Rozwiązanie powinno blokować spam w postaci plików graficznych np. wiadomości z tekstem osadzonym w obrazku. |
| **Kwarantanna Email** | System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako spam z opcją powiadamiania użytkownika.  System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako zainfekowane przez malware.  Rozwiązanie powinno zapewniać możliwość przeglądania kwarantanny z opcją wyszukiwania wiadomości i opcjami filtrowania wraz z opcją zwalniania lub usuwania wiadomości z kwarantanny (przez samoobsługowy portal użytkownika). |
| **Ochrona aplikacji Portalu e-Usług** | Moduł ochrony klasy Web Application Firewall.  Funkcjonalność oparta o mechanizm Reverse Proxy.  Rozwiązanie powinno oferować mechanizm URL hardening with deep-linking and directory traversal prevention.  Rozwiązanie powinno oferować mechanizm Form hardening.  Rozwiązanie powinno oferować ochronę przed SQL injection.  Rozwiązanie powinno oferować ochronę przed Cross-site scripting.  System powinien zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL).  System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.  System powinien pozwalać na podpisywanie plików cookies.  Rozwiązanie powinno oferować wsparcie dla Path-based routing.  Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych.  Rozwiązanie powinno oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing).  System powinien umożliwiać stosowania masek typu wildcard dla ścieżek dostępowych.  System powinien umożliwiać stosowanie operatorów logicznych AND/OR dla reguł. |
|  | System powinien umożliwiać składowanie oraz archiwizację logów w cenie urządzenia.  System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali zagrożenia.  System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.  System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno generować raporty w PDF, HTML i XLS.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 2 serwerów syslog.  System powinien zapewniać podgląd archiwalnego wykorzystania łącza internetowego.  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora. |
| **Certyfikaty** | CE, FCC Class A, CB, VCCI |
| **Subskrypcje** | Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż okres gwarancji. |
| **Gwarancja i wsparcie** | Wsparcie techniczne w trybie 8hx5dni w tygodniu w całym okresie gwarancji. Naprawa bądź wymiana urządzenia NBD (next bussines day).  Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. |

### Kopie zapasowe

Wykonawca w ramach postępowania dostarczy, zainstaluje i wdroży automatyczny system wykonywania kopii bezpieczeństwa zainstalowanych systemów wirtualnych i fizycznych. Wdrożony system kopii bezpieczeństwa musi współpracować w dostarczonym hypervisorem i spełniać następujące parametry:

* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji min. 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
* Oprogramowanie musi być licencjonowanie w modelu “per-CPU” lub „per Serwer”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczone bajty danych, dodatkowo płatna deduplikacja) nie jest dozwolone
* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi posiadać wbudowane mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej dwóch pamięci masowych w takiej puli.
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie ASI wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
* Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage’u produkcyjnego tak aby nie przekraczane były skonfigurowane przez ASI poziomy latencji.
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji
* Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie
* Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
  + **Linux :** ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
  + **Windows :** NTFS, FAT, FAT32, ReFS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
* Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
* Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
* • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
* Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach

## System zarządzania i monitorowania infrastruktury serwerów

System zarządzania infrastrukturą wirtualizacji serwerów musi spełniać następujące kryteria:

1. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
2. Pojedynczy klaster może się skalować min. do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
3. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi obsłużyć   
   i wykorzystać procesory fizyczne wyposażone w min 256 logicznych wątków oraz do min. 8 TB pamięci fizycznej RAM.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych min. od 1 do 64 procesorowych.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do min. 4 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć min. do 10 wirtualnych kart sieciowych.
8. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
11. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 10, Debian GNU/Linux, CentOS, FreeBSD, CoreOS.
12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem HTML.
15. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
16. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
18. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
19. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
20. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
21. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
22. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
23. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
24. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do min. 4000 portów.
25. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
26. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

System monitorowania infrastruktury serwerów wirtualnych musi spełniać następujące kryteria:

* System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
* System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych:
  + Microsoft Windows 2012 R2
  + Microsoft Windows 2016
  + Microsoft Windows 7 z SP1
  + Microsoft Windows 10
* System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:
  + Microsoft SQL Server 2012 R2
  + Microsoft SQL Server 2014
  + Microsoft SQL Server 2016
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej n
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie min. HTML
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
* Silnik raportowania powinien być oparty o SQL w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.0, vCenter Server 5.x oraz 6.0 jak również Microsoft Hyper-V 2012 R2i 2016.
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi instalować się na następujących systemach operacyjnych:
  + Microsoft Windows 7 SP1
  + Microsoft Windows 2012 R2
  + Microsoft Windows 10
  + Microsoft Windows 2016
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
* System musi mieć możliwość eksportowania raportów min. do formatów Microsoft Word, Microsoft Excel, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
* Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić 1 godzinę lub krótszy
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

## Licencje

W ramach postępowania należy dostarczyć wszystkie licencje wymagane do uruchomienia oraz użytkowania dostarczanych urządzeń i serwerów zgodnie z ich przeznaczeniem i niniejszym SIWZ. Licencje terminowe, subskrypcje, abonamenty, itp. muszą pozwalać na użytkowanie każdego elementu Systemu przez okres udzielonej gwarancji od dnia podpisania protokołu odbioru – jeśli dotyczy. Całe oprogramowanie oraz wszystkie licencje muszą być dostarczone w wersjach aktualnych na dzień składania ofert lub nowszych.

Wykonawca określi ilości i rodzaje licencji wymaganych do realizacji Projektu inne niż wymagane, tj.:

* Microsoft Windows Server – zgodnie z warunkami licencjonowania do uruchomienia co najmniej 10 maszyn wirtualnych na wszystkich dostarczonych serwerach fizycznych.
* Licencje CAL AD [device] – 87 szt. – możliwe do zainstalowania w posiadanym przez Zamawiającego systemie Active Directory.
* System kopii bezpieczeństwa – zgodnie z warunkami licencjonowania do wykonywania kopii bezpieczeństwa wszystkich zainstalowanych systemów [zarówno fizycznych jak i wirtualnych].
* System wirtualizacji – zgodnie z warunkami licencjonowania do uruchomienia co najmniej 100 maszyn wirtualnych na wszystkich dostarczonych serwerach.

# Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego

Wszystkie dostarczane urządzenia muszą zostać zainstalowane [tj. wypakowane, zmontowane, zamontowane w szafach rack lub na biurkach, uruchomione i skonfigurowane] w docelowym miejscu pracy [wskazanym przez Zamawiającego] w terminie wskazanym przez Zamawiającego [miejsce i termin instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń]. Wszystkie opakowania zostaną zutylizowane przez i na koszt Wykonawcy.

**Wszystkie urządzenia i systemy operacyjne serwerów muszą być zsynchronizowane z lokalnym serwerem czasu.**

Serwery, macierz, firewall, UPS oraz wszystkie inne dostarczone w ramach tego postępowania urządzenia przeznaczone do instalacji w szafie RACK, muszą być zainstalowane w szafie RACK. Jeżeli dostarczony sprzęt nie będzie mógł być zainstalowany w istniejących u Zamawiającego szafach RACK, Wykonawca dostarczy szafę RACK 19” 42U o parametrach minimalnych pozwalających na pracę wszystkich urządzeń zgodnie z wytycznymi producentów oferowanego sprzętu.

## Serwery

Na serwerach należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy w możliwie najszybszy sposób. Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia. Wykonawca zaprojektuje i wdroży system backupu min. maszyn wirtualnych.

## Macierz dyskowa

Macierz musi zostać zainstalowana w serwerowni. Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób.

## Serwer Kopii Zapasowych

Serwer kopii zapasowych musi zostać zainstalowany w serwerowni. Zasoby serwera kopii posłużyć mają do przechowywania dodatkowych kopii bezpieczeństwa systemów zainstalowanych w serwerowni. Serwer musi zostać podłączony do sieci wewnątrz serwerowej.

## Zasilanie awaryjne – UPS

UPS musi posiadać aktywną kartę sieciową pozwalającą na monitorowania za pomocą min.: Interfejsu WEB oraz protokołu SNMP w wersji 2 oraz 3. UPS musi zostać skonfigurowany w taki sposób, aby w przypadku zaniku napięcia w sieci energetycznej wysyłana była wiadomość e-mail do ASI oraz aby rejestrowany był ten fakt w centralnym systemie logów lub systemie monitorowania serwerów i usług za pomocą SNMP Trap [włącznie z informacją o przywróceniu napięcia]. Dodatkowo za pomocą SNMP traps rejestrowane muszą być wszystkie inne zdarzenia mogące mieć wpływ na działanie systemów i ich bezpieczeństwo [np. konieczność wymiany baterii czy przeciążenie]. W systemie zarządzania należy utworzyć dwóch użytkowników z prawami administracyjnymi [jeden dla ASI, jeden dla serwisu]. Jeśli interfejs posiada konto „gościa” należy je wyłączyć. Wszystkie możliwe protokoły sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepowołanym dostępem. UPS musi zostać zainstalowany w szafie RACK w przeznaczony przez producenta do tego celu sposób [np. za pomocą odpowiednich szyn lub uchwytów]. UPS musi zostać podłączony do sieci LAN poprzez dedykowany interfejs zarządzania do odpowiedniego portu na przełączniku sieciowym [odpowiedni vlan!]

## Stanowiska robocze

Konfiguracja urządzeń polegać będzie na:

* wypakowaniu urządzenia z opakowania,
* podłączeniu fizycznym do sieci LAN oraz elektrycznej,
* podłączenie do domeny Active Directory,
* skonfigurowaniu adresu IP w systemie kontroli ruchu sieciowego – jeśli wymagane,
* konfiguracji interfejsu zarządzania [jeśli posiada], konfiguracji synchronizacji z lokalnym serwerem czasu.

## Zabezpieczenie e-Usług

Wykonawca dokona instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.

Wykonawca wdroży [tj. zainstaluje, uruchomi, skonfiguruje i przetestuje] infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerze fizycznym Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem [np. Active Directory, DHCP, DNS, SQL, IIS, etc.].

### Firewall – UTM

W konfiguracji urządzeń muszą zostać włączone min. usługi:

* ochrony przed atakami typu DoS/DDoS, itp.,
* ochrony antywirusowej,
* web filter,
* IDS/IPS.

Uruchomiony Firewall musi zostać skonfigurowany w taki sposób, aby jednostki terenowe łączyły się z centralą za pośrednictwem bezpiecznego kanału transmisji – VPN.

Instalowane urządzenie musi chronić zainstalowane wewnątrz sieci Zamawiającego serwery aplikacyjne e-Usług [głównie przed atakami typu DoS, sql-injection, itp].

### Kopie zapasowe

Wykonawca we współpracy z ASI opracuje politykę kopii bezpieczeństwa uwzględniającą możliwości techniczne po wdrożeniu Projektu. Na podstawie polityki Wykonawca skonfiguruje systemy i usługi do wykonywania kopii bezpieczeństwa zgodnie z harmonogramami. Przetestuje działanie mechanizmu automatycznego wykonywania kopii bezpieczeństwa i po okresie 30 dni od uruchomienia harmonogramu oceni skuteczność wdrożonych mechanizmów. W ramach wdrożenia musi zostać dostarczona instrukcja odtwarzania danych w różnych zakresach [np.: pojedynczy plik, cały katalog, użytkownik wraz z plikami, maszyna, itp.]. Wszystkie kopie muszą być zapisywane min. na serwerze kopii – zgodnie ze złożoną ofertą.

### Architektura HA dla serwera aplikacji

W celu zapewnienia wysokiej dostępności e-Usług należy uruchomić wirtualne serwery aplikacji w trybie HA. W celu wyeliminowania pojedynczego punktu awarii (jeśli zostanie zastosowany serwer load-balancera) usługa load-balancing’u również musi zostać uruchomiona w trybie HA (np. z wykorzystaniem DNS round-robin). W celu zapewnienia rozliczalności danych w trybie HA muszą zostać uruchomione zarówno serwery load-balancing’u oraz aplikacji jak i e-Usług. Wykonawca może zaproponować inne rozwiązanie gwarantujące równie wysoką dostępność.

### Architektura HA dla serwera bazy danych

Serwer bazy danych systemu e-Usług musi zostać zabezpieczony na wypadek awarii zarówno serwera wirtualnego jak i fizycznego. Dlatego instancja serwera SQL musi zostać uruchomiona w trybie HA. Zamawiający nie stawia wymogu zastosowania konkretnej technologii czy konkretnego rozwiązania, wymaga jedynie spełnienie funkcjonalności w tym zakresie. Podstawowy serwer bazy danych musi zostać skonfigurowany w sposób maksymalizujący szybkość działania systemu bazodanowego [np.: podział dysków na grupy RAID, przeniesienie logów na oddzielne dyski, itp.]. Serwer zapasowy musi się uruchomić najwyżej w ciągu 1 minuty i przejąć rolę serwera podstawowego. Po przywróceniu działania serwera podstawowego powinien stać on się serwerem zapasowym lub jeśli będzie oferował lepszą wydajność powinien zostać wypromowany jako serwer podstawowy bez przerwy w działaniu usług.

### Usługi wspomagające

#### DNS

Należy uruchomić min. dwa serwery DNS działające w trybie HA i skonfigurować wszystkie niezbędne usługi – w tym round-robin dla load balancerów. Usługa DNS musi posiadać możliwość włączenia filtrowania kategorii stron internetowych, których adresy system DNS będzie zwracał.

#### NTP

Należy uruchomić min. dwa serwery NTP działające w trybie HA lub wzajemnej synchronizacji i skonfigurować wszystkie usługi i urządzenia do korzystania z tych serwerów.

#### Aplikacja TESTOWA

W szczególności do celów podnoszenia kompetencji i samokształcenia personelu, należy uruchomić dodatkowe serwery Testowych instancji e-Usług [aplikacji i bazy danych].

# Zakres 3 – Przygotowanie oraz przeprowadzenie szkoleń w zakresie użytkowania i administrowania dostarczonym sprzętem i oprogramowaniem

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu administrowania zainstalowanymi Systemami na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia.

Szkolenia z użytkowania i administracji Systemu dla administratorów systemu (min. 3 osoby).

Szkolenia są niezbędne w celu zagwarantowania osiągnięcia zakładanych efektów w projekcie.

Szczegółowy zakres poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiający w ramach akceptacji harmonogramu i materiałów szkoleniowych.

Do każdego modułu wspomagającego obsługę obszarów działalności, Zamawiający wskaże osoby, które Wykonawca przeszkoli.

Jeśli do przeprowadzenia szkolenia będzie wymagany dodatkowy sprzęt, Wykonawca zobowiązany jest go zapewnić na czas szkolenia.

Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych – dopuszcza prowadzenie szkoleń e-learningowych jedynie w ramach szkoleń uzupełniających.

Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 20 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych – dot. szkoleń certyfikowanych wyjazdowych.

W przypadku konieczności zorganizowania szkolenia poza siedzibą Zamawiającego – np. szkolenia certyfikowane producenta – Wykonawca pokryje koszty przejazdu, zakwaterowania i wyżywienia osób skierowanych na szkolenia (max 3 osoby).

Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiającego w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.

Wykonawca zapewni przeszkolenie administratorów wskazanych przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanych systemów i rozwiązań informatycznych. Szkolenie musi obejmować co najmniej instalację, konfigurację, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.

Uzgodnieniu pomiędzy stornami podlegają:

* Poziom szkoleń w zależności od wiedzy i umiejętności osób skierowanych na szkolenia,
* Harmonogram szkoleń grupowych i indywidualnych,
* Materiały szkoleniowe dla szkoleń grupowych,
* Listy obecności ze szkoleń grupowych i indywidualnych,
* Protokoły odbioru zadania dot. szkoleń.

Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać pracownikom na rozpoczęcie pracy w systemie.

Zamawiający wymaga aby szkolenia z zakresu administrowania oprogramowaniem wirtualizacji serwerów były certyfikowanymi szkoleniami producenta lub certyfikowanej jednostki szkoleniowej.

# Zakres 4 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył instrukcję dostępu do systemów i sieci Internet [LAN oraz WLAN] zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów/urządzeń.

Dokumentacja musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści.

# Zakres 5 – Gwarancja i wsparcie

Świadczenie usługi gwarancji i wsparcia ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp. Zakres i warunki opisane w Załączniku nr 6 do Umowy.

Wykonawca zobowiązuje się do dostarczania wolnych od wad kolejnych wersji Systemu.

Wykonawca zobowiązuje się do aktualizacji dokumentacji Użytkownika i/lub Administratora.

Wykonawca zobowiązuję się do świadczenia konsultacji dla Administratorów w zakresie niezbędnych zmian w konfiguracji systemu.

Wykonawca zapewni usługę wsparcia użytkowników udostępniając:

* + usługę typu helpdesk, udostępnioną pod adresem e-mail, numerem telefonu
  + portal typu helpdesk – dostępny on-line w trybie 356/7/24, gdzie będą publikowane m.in. statusy zgłoszeń oraz ich treść i historia korespondencji
  + przez niniejszy portal będą mogły być dokonywane zgłoszenia Dysfunkcji

Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy systemu zgodnego z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Administratorów związane z bieżącą eksploatacją Systemu.

Wykonawca zapewni w godzinach pracy Zamawiającego w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów.

Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.

Wykonawca będzie świadczył na rzecz Zamawiającego usługi serwisu w zakresie przedmiotu zamówienia (umowy) w zaoferowanym w postępowaniu okresie (licząc od daty podpisania protokołu odbioru) zapewniając jednocześnie odpowiednie wsparcie merytoryczne.

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

* + z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: Dysfunkcji w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
  + związanych z realizacją usługi wdrożenia Systemu;
  + spowodowanych aktualizacjami Systemu.

Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów.

Zgłaszający, w przypadku wystąpienia dysfunkcji przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia Dysfunkcji. W Zgłoszeniu powinny być wypełnione wszystkie obligatoryjne pola formularza, a opis sytuacji prowadzącej do wystąpienia błędu lub awarii powinien umożliwiać jej odtworzenie przez zespół serwisowy Wykonawcy. Jeżeli odtworzenie błędu nie będzie możliwe w środowisku Wykonawcy, wówczas zdiagnozuje on błąd w środowisku Zamawiającego, a terminy usunięcia Dysfunkcji ulegają wydłużeniu o czas oczekiwania na dostęp do środowiska Zamawiającego.

Wykonawca zobowiązany jest do potwierdzenia w ciągu 4 godzin przyjęcie Zgłoszenia oraz jego klasyfikację. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.

Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie.

Zgłoszenia będą klasyfikowane zgodne ze słownikiem pojęć, zawartym w Załączniku nr 6 do Umowy, przez Zamawiającego w uzgodnieniu z Wykonawcą.

Wykonawca zobowiązany jest do usunięcia dysfunkcji w terminach wymienionych w pkt 7 procedury podejmowania prac serwisowych zawartej w Załączniku nr 6 do Umowy.

W każdym przypadku Zgłaszający i Wykonawca mogą uzgodnić inny czas dostarczenia rozwiązania niż określono w warunkach gwarancji. W takim przypadku niezbędne jest potwierdzenie ustalonego terminu w formie pisemnej, faksem lub e-mailem.

Terminy wymienione w Załączniku nr 6 do Umowy obowiązują również w przypadku dostarczonego sprzętu.

1. Od podpisania umowy [↑](#footnote-ref-1)
2. Od zakończenia dostaw sprzętu [↑](#footnote-ref-2)
3. Na całość rozwiązania od momentu podpisania ostatniego Protokołu Odbioru Końcowego Zakresów od 1 do 4 – termin zgodnie z ofertą. [↑](#footnote-ref-3)
4. Parametr ważny z uwagi na docelowe wykorzystanie serwera [↑](#footnote-ref-4)