***Załącznik nr ….***

**Szczegółowy Opis Przedmiotu Zamówienia**

Dostawa i wdrożenie sprzętu serwerowego wraz z oprogramowaniem systemowym i narzędziowym w ramach projektu pn. „ Zwiększenie dostępności e-usług dla miasta Starachowice”

Spis treści

[Spis treści 2](#_Toc129168076)

[Rozdział I. Założenia początkowe oraz wymagania ogólne 3](#_Toc129168077)

[I.1 Wprowadzenie 3](#_Toc129168078)

[I.2 Ogólny opis przedmiotu zamówienia 3](#_Toc129168079)

[I.3 Termin realizacji Przedmiotu Zamówienia 5](#_Toc129168080)

[I.4 Organizacja wdrożenia 5](#_Toc129168081)

[**I.4.1** **Założenia podstawowe** 5](#_Toc129168082)

[**I.4.2** **Przygotowanie Dokumentacji** 6](#_Toc129168083)

[**I.4.3** **Harmonogram wdrożenia** 7](#_Toc129168084)

[**I.4.4** **Analiza Przedwdrożeniowa** 7](#_Toc129168085)

[**I.4.5** **Dokumentacja Powykonawcza** 7](#_Toc129168086)

[**I.4.6** **Odbiór Etapu/Dokumentacji/Końcowy** 8](#_Toc129168087)

[**I.4.7** **Dostawa i instalacja oprogramowania standardowego** 9](#_Toc129168088)

[**I.4.8** **Testy** 9](#_Toc129168089)

[**I.4.9** **Dodatkowe zobowiązania Wykonawcy** 9](#_Toc129168090)

[Rozdział II. Szczegółowy opis przedmiotu zamówienia 10](#_Toc129168091)

[II.1 Dostawa i wdrożenie Infrastruktury Serwerowej 10](#_Toc129168092)

[**II.1.1** **Serwer wirtualizacji produkcyjny** 11](#_Toc129168093)

[**II.1.2** **Serwer backupu** 12](#_Toc129168094)

[**II.1.3** **Macierz dyskowa** 14](#_Toc129168095)

[**II.1.4** **Półka dyskowa** 16](#_Toc129168096)

[**II.1.5** **Macierz dyskowa - aktualizacja** 16](#_Toc129168097)

[II.2 Oprogramowanie systemowe i narzędziowe 17](#_Toc129168098)

[**II.2.1** **Licencje oprogramowania wirtualizacji klastra dziedzinowego oraz wirtualizacji stacji roboczych (klaster podstawowy i zapasowy)** 17](#_Toc129168099)

[**II.2.2** **Licencje systemu operacyjnego serwera wirtualizacji** 20](#_Toc129168100)

[**II.2.3** **Licencje systemu operacyjnego serwera backupu** 23](#_Toc129168101)

[**II.2.4** **Licencje systemu antywirusowego** 25](#_Toc129168102)

[**II.2.5** **Licencje systemu backupu** 33](#_Toc129168103)

[II.3 Usługi w zakresie infrastruktury serwerowej i terminalowej 34](#_Toc129168104)

[**II.3.1** **Usługi – klaster wirtualizacyjny stacji roboczych** 34](#_Toc129168105)

[**II.3.2** **Usługi – klaster dziedzinowy** 36](#_Toc129168106)

[**II.3.1** **Instruktaże/ warsztaty** 37](#_Toc129168107)

[Rozdział III. Gwarancja 38](#_Toc129168108)

[III.1 Okres gwarancji 38](#_Toc129168109)

[III.2 Reżimy realizacji usług serwisowych 39](#_Toc129168110)

[III.3 Pozostałe ustalenia 40](#_Toc129168111)

# Założenia początkowe oraz wymagania ogólne

## Wprowadzenie

1. Przedmiot zamówienia jest realizowany w ramach Projektu pn. „Zwiększenie dostępności e-usług dla miasta Starachowice” współfinansowanego ze środków Unii Europejskiej z Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2014-2020, VII Oś Priorytetowa: Sprawne usługi publiczne Działanie 7.1: Rozwój e-społeczeństwa.
2. Głównym cel zadań jest wzrost upowszechnienia wykorzystania technik informacyjnych i komunikacyjnych w usługach publicznych on-line dotyczących administracji publicznej samorządu Starachowic.
3. Wszystkie działania zaplanowane w zadaniach będą służyć realizacji celu poprzez zwiększenie dostępności lub dojrzałości usług publicznych świadczonych drogą elektroniczną, utworzenie lub poprawę warunków techniczno-organizacyjnych do obsługi tych usług.

## Ogólny opis przedmiotu zamówienia

1. Przedmiot zamówienia obejmuje**:**
   1. **Infrastruktura serwerowa w zakresie:**

|  |  |  |
| --- | --- | --- |
| **Pozycja OPZ** | **Opis** | **Ilość** |
| **Rozdział II.1** | **Infrastruktura serwerowa** | **szt.** |
| II.1.1 | Serwer wirtualizacji - produkcyjny | 4 |
| II.1.2 | Serwer backupu | 1 |
| II.1.3 | Macierz dyskowa | 1 |
| II.1.4 | Półka dyskowa | 2 |
| II.1.5 | Macierz dyskowa - aktualizacja | 1 |

* 1. **Oprogramowanie systemowe i narzędziowe w zakresie:**

|  |  |  |
| --- | --- | --- |
| **Pozycja OPZ** | **Opis** | **Ilość** |
| **Rozdział II.2** | **Oprogramowanie systemowe i narzędziowe** | **szt.** |
| II.2.1 | Licencje oprogramowania wirtualizacji klastra dziedzinowego oraz wirtualizacji stacji roboczych (klaster podstawowy i zapasowy) | 1 kpl. |
| II.2.2 | Licencje systemu operacyjnego serwera wirtualizacji | 1 kpl. |
| II.2.3 | Licencje systemu operacyjnego serwera backupu | 1 kpl. |
| II.2.4 | Licencje systemu antywirusowego | 1 kpl. |
| II.2.5 | Licencje systemu backupu | 1 kpl. |

* 1. **Usługi w zakresie infrastruktury i oprogramowania**:

|  |  |
| --- | --- |
| **Pozycja OPZ** | **Opis** |
| **Rozdział II.3** | **Usługi** |
| II.3.1 | Usługi – klaster wirtualizacji stacji roboczych |
| II.3.2 | Usługi – klaster dziedzinowy |
| II.3.3 | Instruktaże/warsztaty |

1. Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego z ustalonym podziałem na serwerownię podstawową i rezerwową:

Serwerownia podstawowa: ul. Leśna 2 (budynek dawnego Gimnazjum nr 3)

Serwerownia rezerwowa: ul. Radomska 45

1. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
2. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
3. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Umowy.
4. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza rozwiązanie równoważne opisywanym w treści SWZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza składanie ofert na rozwiązania równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w+ stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.
5. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia lub elementu, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
6. Wszelkie dostarczane urządzenia:
7. muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta oraz muszą reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń odnawianych, demonstracyjnych lub powystawowych.
8. nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta,
9. elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub muszą być przez niego certyfikowane oraz w całości muszą być objęte gwarancją producenta,
10. urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta,
11. urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta,
12. do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim, w formie papierowej lub elektronicznej,

## Termin realizacji Przedmiotu Zamówienia

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 3 miesięcy od daty zawarcia umowy.

## Organizacja wdrożenia

* + 1. **Założenia podstawowe**

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram wdrożenia w terminie 14 dni od daty podpisania umowy.
2. Wykonawca w Harmonogramie wdrożenia musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich realizowanych przez niego pracach w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.
5. Wykonawca zobowiązany jest przeprowadzić dostawy przedmiotu zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. Dostarczana Infrastruktura musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i p3roducenta. Ponadto, infrastruktura, o której mowa musi pochodzić z oficjalnych kanałów dystrybucji producentów oraz musi być dostarczona w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie przedmiotu zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
9. W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:
10. Kierownik Projektu ze strony Wykonawcy,
11. Zespół Wdrożeniowy ze strony Wykonawcy.
12. Wdrożenie, z zastrzeżeniami wskazanymi poniżej muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
13. Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
14. Wykonawca musi przekazać Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.
    * 1. **Przygotowanie Dokumentacji**
15. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia(zwaną dalej Dokumentacją), która składa się z nw. zakresów:
16. Harmonogram Wdrożenia,
17. Dokumentacja Analizy Przedwdrożeniowej (DAP),
18. Dokumentacja Powykonawcza.
19. Dokumentacja powyższa musi zawierać bazowe zapisy opisujące budowane rozwiązania oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach przedmiotu zamówienia. Dokumenty te wraz ze SWZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
20. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
21. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia muszą być opracowane w oparciu o wymagania określone w niniejszym OPZ.
    * 1. **Analiza Przedwdrożeniowa**

Analiza Przedwdrożeniowa obejmuje wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie środowiska informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP) oraz harmonogram wdrożenia, na podstawie której organizacyjnie i technicznie będzie realizowany przedmiot zamówienia. DAP będzie podlegała uzgodnieniu i akceptacji Zamawiającego. Termin wykonania analizy został określony w umowie.

1. DAP musi zawierać w szczególności:

|  |
| --- |
| **ZawarTość Dokumentacji Analizy Przedwdrożeniowej DAP** |
| 1. **Wymagane dane ZARZĄDCZE:** |
| 1. plan i sposób komunikacji Stron. |
| 1. harmonogram wdrożenia |
| 1. **Wymagane dane dotyczące INFRASTRUKTURY SERWEROWEJ:** |
| 1. podział przedmiotu zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty, |
| 1. analiza wymagań przedmiotu zamówienia zawierająca opis sposobu realizacji wymagań, sposób testowania i odbioru, |
| 1. karty katalogowe urządzeń potwierdzające spełnienie wymagań, |
| 1. plan dostaw, |
| 1. opis prac w zakresie sieci teleinformatycznej, |
| 1. opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą serwerową, |
| 1. opis prac w zakresie budowy Infrastruktury serwerowej, |
| 1. lista Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy, |
| 1. szczegółowy zakres i zawartość pozostałej Dokumentacji. |

* + 1. **Dokumentacja Powykonawcza**

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta musi zawierać:

#### Wymogi ogólne:

1. opis architektury technicznej,
2. konfiguracja musi obejmować wszystkie wdrożone urządzenia, zainstalowane w ramach budowy systemu IT,
3. przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:
   * serwery – parametry sprzętowe (procesor, pamięć, dyski, karty sieciowe, zasilanie, itp.),
   * sieć (adresacja IP, itp.),
   * podsystem dyskowy (punkty montowania/litery dysków, wolumeny logiczne, grupy wolumenowe, zasoby dyskowe, RAID, itp.),
   * system operacyjny (parametry jądra, moduły, usługi, stos TCP/IP, itp.),
   * klaster (węzły fizyczne, paczki klastrowe, kolejność przełączania, itp.),
   * listę zainstalowanego oprogramowania, itp.,
   * macierze – parametry sprzętowe (cache, półki dyskowe, dyski, karty/porty fibre channel, itp.), grupy dyskowe, zasoby dyskowe, maskowanie, kopie biznesowe, replikacja, itp.,
4. opis wymagań sprzętowych, systemowych, sieciowych itp.

* wymagania dla poszczególnych komponentów architektury, odniesienia do oczekiwanych wymagań wydajnościowych, funkcjonalnych i bezpieczeństwa (minimalny, maksymalny, rekomendowany),

1. procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji.

* szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców dla standardowych komponentów (np. baz danych) wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów,

1. dokumenty z testów:

* plan testów, scenariusze testowe i protokoły z testów akceptacyjnych, wydajnościowych, testów operacji administratora technicznego oraz testów bezpieczeństwa w tym ciągłości działania (przełączanie, odtwarzanie, weryfikacja poprawności),
  + 1. **Odbiór Etapu/Dokumentacji/Końcowy**

1. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
2. Odbiór końcowy przedmiotu zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
3. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej załącznik nr ….. do SWZ.
   * 1. **Dostawa i instalacja oprogramowania standardowego**
4. Oprogramowanie standardowe rozumiane jako oprogramowanie dostarczone i zainstalowane na Infrastrukturze serwerowej posiadanej przez Zamawiającego lub dostarczane zgodnie z Umową stanowiącą załącznik nr … do SWZ oraz w istniejących systemach informatycznych zgodnie z wymaganiami niniejszego Opisu Przedmiotu Zamówienia musi zapewniać prawidłowe funkcjonowanie sprzętu oraz istniejących systemów informatycznych na wszystkich stanowiskach pracy (stanowiskach komputerowych) Zamawiającego.
5. Dostawa i instalacja zostaną wykonane w lokalizacjach zgodnych z instalacją urządzeń   
   u Zamawiającego i zgodnie z Harmonogramem wdrożenia.
6. Oprogramowanie standardowe musi zostać skonfigurowane tak, aby działało poprawnie zgodnie z jego przeznaczeniem i architekturą Systemu.
   * 1. **Testy**
7. W ramach odbioru przedmiotu zamówienia muszą zostać przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.
8. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego przedmiotu zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru Końcowego.
9. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
10. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.
    * 1. **Dodatkowe zobowiązania Wykonawcy**
11. Wykonanie przedmiotu zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
12. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres   
    i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
13. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
14. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
15. Współdziałanie z osobami wskazanymi przez Zamawiającego.

# Szczegółowy opis przedmiotu zamówienia

## Dostawa i wdrożenie Infrastruktury Serwerowej

1. Wykonawca zobowiązany jest dostarczyć i uruchomić kompleksową platformę Infrastruktury serwerowej (serwery, macierze wraz z niezbędnym Oprogramowaniem Narzędziowym – systemowym, wirtualizacyjnym i pozostałym oprogramowaniem).
2. Dostawa i instalacja zostaną wykonane w lokalizacjach Zamawiającego zgodnie z Harmonogramem wdrożenia.
3. Infrastruktura musi być dostarczona do Zamawiającego, w terminie ustalonym z upoważnionym przedstawicielem Zamawiającego.
4. Jeżeli zajdzie potrzeba, wraz z dostarczoną Infrastrukturą, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu jej do sieci informatycznej Zamawiającego.
5. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
6. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.
7. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury zostaną ustalone w trakcie Analizy Przedwdrożeniowej.
8. Zamawiający wymaga odbycia wizji lokalnej Wykonawcy, Wizja lokalna może odbyć się w pracujące dni powszednie (poniedziałek – piątek) w zakresie godzin od 8:00 do 15:00 po uzgodnieniu konkretnego terminu z Zamawiającym.
9. Wykonawcy, którzy są zainteresowani przeprowadzeniem ww. wizji lokalnej w celu zapoznania się z środowiskiem Zamawiającego, zobowiązani są zgłosić chęć uczestniczenia w wizji lokalnej za pośrednictwem skrzynki elektronicznej: [zamowienia@starachowice.eu](mailto:zamowienia@starachowice.eu) . O terminie przeprowadzenia wizji lokalnej Wykonawcy zostanie poinformowany mailem.
10. Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, wirtualizacyjnego itd.) wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji.
11. Wykonawca zobowiązany jest zapewnić 60 miesięczne wsparcie i możliwość prowadzenia konsultacji w zakresie administracji zaoferowanym sprzętem oraz dostarczonym oprogramowaniem narzędziowym (systemowym i wirtualizacyjnym) z osobami wskazanymi przez Wykonawcę, posiadającymi odpowiednie certyfikaty producentów urządzeń i oprogramowania na warunkach gwarancji producenta lub dostawcy sprzętu. Pozostałe wymagania dotyczące gwarancji zostały opisane w OPZ w rozdziale III. Gwarancja.
12. Wszystkie urządzenia muszą być fabrycznie nowe - na dzień dostawy sprzęt nie może być starszy niż 9 miesięcy.
    * 1. **Serwer wirtualizacji produkcyjny**

Wymagane jest dostarczenie 4 szt. serwerów spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Obudowa** | Obudowa Rack o wysokości max 2U.  Wraz z zestawem montażowym RACK i zestawem organizacji okablowania.  Wyświetlacz LCD lub zestaw diod sygnalizacyjnych na przednim panelu serwera. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.  Zainstalowany moduł TPM 2.0. |
| **Procesor** | Wyposażony w maksymalnie dwa fizyczne procesory, posiadające łącznie nie więcej niż 32 fizycznych rdzeni  Wydajność rodziny oferowanych serwerów z zaoferowanymi procesorami w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org musi wynosić min. 262 pkt, przy konfiguracji dwuprocesorowej.  Parametry procesora ograniczone w związku z licencjonowaniem użytkowanego na nim oprogramowania. Zainstalowane procesory powinny umożliwiać konfigurację klastra platformy wirtualizacyjnej Vmware vSphere z posiadanymi przez Zamawiającego serwerami wyposażonymi w procesory firmy Intel. |
| **RAM** | Minimum 768GB DDR4 RDIMM 3200MT/s lub wydajniejsze.  Płyta główna powinna obsługiwać do min. 8TB pamięci RAM.  Pamięć zorganizowana w modułach o pojemności min. 64GB. |
| **Złącza PCI** | Oferowane urządzenie musi być wyposażone w złącza kart rozszerzeń PCIe generacji 4. |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT niezajmujące slotu kart rozszerzeń PCIe, tj.: dwa porty trwale zintegrowane z płytą główną lub dwuportowa karta sieciowa wykorzystująca dedykowany port rozszerzeń (np. OCP 3.0, NDC).  Dwie dodatkowe karty dwuportowe SFP28 10/25Gb, w tym minimum jedna musi wspierać protokół RDMA. |
| **Dyski twarde** | Zainstalowane 2 nośniki typu dyski SSD o pojemności min.480GB lub flash o odpowiedniej pojemności.  Rozwiązanie RAID wspierane minimum przez oprogramowanie Vmware ESXi 6.7, 7.0 i 8.0, jak również Microsoft Windows Server 2019 oraz Microsoft Windows Server 2022. |
| **Zasilacze** | Redundantne, Hot-Plug min. 1400W. |
| **Video** | Zintegrowana karta graficzna |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * zdalne monitorowanie i informowanie o statusie serwera * szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH * integracja z Active Directory * możliwość obsługi przez dwóch administratorów jednocześnie * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * Automatyczne update firmware dla wszystkich komponentów serwera. * Możliwość przywrócenia poprzednich wersji firmware. * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych. |
| **System operacyjny - zgodność** | Posiadające pełną zgodność i wsparcie dla następujących systemów operacyjnych: Microsoft Windows Server 2016, 2019, 2022, Linux SuSE, Linux RedHat, Vmware vSphere 6.7, 7.0 i 8.0.  Serwer musi znajdować się na liście zgodności dla systemu VMwareESXi8.0 zamieszczonej na stronie: https://www.vmware.com/resources/compatibility/search.php? |
| **Certyfikaty** | Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Windows Serwer 2022 minimum w zakresie „Software-Defined Data Center (SDDC) Premium”.  ISO-9001 oraz ISO-14001.  Deklaracja CE. |
| **Warunki gwarancji** | 60 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość sprawdzenia u producenta na jego stronie internetowej lub telefonicznie na infolinii producenta prowadzonej w języku polskim, konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego urządzenia.  W zakresie wsparcia i gwarancji Zamawiający wymaga przedstawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta oraz, że uszkodzone dyski w przypadku wymiany z powodu awarii w okresie obowiązywania gwarancji, pozostaną własnością Zamawiającego. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą. |

* + 1. **Serwer backupu**

Wymagane jest dostarczenie 1 szt. serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Obudowa** | Obudowa Rack o wysokości max 2U, z możliwością instalacji minimum 12 dysków 3.5" oraz 2 dysków 2,5”  Wraz z zestawem montażowym RACK i zestawem organizacji okablowania.  Wyświetlacz LCD lub zestaw diod sygnalizacyjnych na przednim panelu serwera. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.  Zainstalowany moduł TPM 2.0. |
| **Procesor** | Wyposażony w maksymalnie dwa fizyczne procesory, posiadające łącznie nie więcej niż 16 fizycznych rdzeni  Wydajność rodziny oferowanych serwerów z zaoferowanymi procesorami w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org musi wynosić min. 130 pkt, przy konfiguracji dwuprocesorowej.  Parametry procesora ograniczone w związku z licencjonowaniem użytkowanego na nim oprogramowania. |
| **RAM** | Minimum 128GB DDR4 RDIMM 3200MT/s lub wydajniejsze.  Płyta główna powinna obsługiwać min. 1TB pamięci RAM. |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  Dwie dodatkowe karty dwuportowe SFP28 10/25Gb. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy RAID z minimum 4 GB pamięci, możliwe konfiguracje poziomów RAID : 1, 5, 6.  Szybkość transmisji danych: 12 Gbps |
| **Dyski twarde** | Zainstalowane:  - Zainstalowane 2 nośniki typu dyski SSD o pojemności min.480GB  - 12 szt. dysków NLSAS 7.2K RPM 12Gbps, o pojemności minimum 8TB każdy |
| **Zasilacze** | Redundantne, Hot-Plug min. 750W. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:  • zdalny dostęp do graficznego interfejsu Web karty zarządzającej  • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera)  • szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika  • możliwość podmontowania zdalnych wirtualnych napędów  • wirtualną konsolę z dostępem do myszy, klawiatury  • wsparcie dla IPv6  • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH  • integracja z Active Directory  • możliwość obsługi przez dwóch administratorów jednocześnie  • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  • Automatyczne update firmware dla wszystkich komponentów serwera.  • Możliwość przywrócenia poprzednich wersji firmware.  • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON  • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych. |
| **System operacyjny - zgodność** | Posiadające pełną zgodność i wsparcie dla następujących systemów operacyjnych: Microsoft Windows Server 2016, 2019, 2022, Linux SuSE, Linux RedHat, Vmware vSphere 6.7, 7.0 i 8.0. |
| **Certyfikaty** | Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Windows Serwer 2022 minimum w zakresie „Software-Defined Data Center (SDDC) Premium”  ISO-9001 oraz ISO-14001.  Deklaracja CE. |
| **Warunki gwarancji** | 60 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość sprawdzenia u producent na jego stronie internetowej lub telefonicznie na infolinii producenta prowadzonej w języku polskim, konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego urządzenia.  W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta oraz, że uszkodzone dyski w przypadku wymiany z powodu awarii w okresie obowiązywania gwarancji, pozostaną własnością Zamawiającego. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą. |

* + 1. **Macierz dyskowa**

Wymagane jest dostarczenie 1 szt. macierzy spełniających poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Kompatybilność** | Zamawiający posiada macierz dyskową DELL EMC Unity XT 380 – posiadająca następujące wyposażenie:  Dyski: 23x 1.8 TB SAS 10k, 2x 400 GB FLASH SSD  Porty komunikacyjne po stronie Hostów: 4x FC 16Gb/s, 8x 25 Gb/s  Zamawiający wymaga, aby oferowana macierz dyskowa umożliwiała skonfigurowanie replikacji synchronicznej i asynchronicznej dla danych blokowych z posiadaną przez Zamawiającego macierzą DELL EMC Unity XT 380 w celu stworzenia rozwiązania wysokiej dostępności.  Zaoferowane rozwiązanie musi posiadać architekturę i zostać dostarczone w konfiguracji, która wspiera migrowanie maszyn wirtualnych pomiędzy ośrodkami w oparciu o replikacje synchroniczną z wykorzystaniem protokołu FC dla danych blokowych. W przypadku awarii jednego z ośrodków nastąpi przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana w oparciu o funkcjonalność macierzy dyskowych i dostarczanego w ramach niniejszego postępowania oprogramowania do automatyzacji przełączania maszyn wirtualnych.  Jeżeli ta funkcjonalność wymaga licencji to należy ją dostarczyć.  Zamawiający wymaga wdrożenia replikacji blokowej z posiadaną przez Zamawiającego macierzą DELL EMC Unity XT 380.  Zamawiający dopuszcza w przypadku braku możliwości zrealizowania rozwiązania wysokiej dostępności w oparciu o replikację synchroniczną i asynchroniczną z posiadaną macierzą dyskową, jako rozwiązanie równoważne dostarczenie dwóch macierzy dyskowych, z których każda musi w pełni spełnić zapisy niniejszego OPZ oraz zapewniających możliwość zrealizowania architektury wysokiej dostępności, takiej jak opisana w niniejszym punkcie, wraz z narzędziem do migracji danych blokowych pomiędzy tymi macierzami, a macierzą posiadaną przez Zamawiającego, wspieranym oficjalnie przez producenta posiadanej przez Zamawiającego macierzy dyskowej, obsługiwanym z interfejsu graficznego. |
| **Obudowa** | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.  Musi posiadać możliwość rozbudowy do minimum 400 dysków w jednym systemie macierzowym sterowanym przez dostarczoną parę kontrolerów.  Musi posiadać możliwość rozbudowy o półkę dyskową umożliwiające instalację dodatkowych dysków 2,5” i 3,5”. |
| **Architektura** | Macierz wyposażona w dwa fizyczne kontrolery pracujące w trybie active/active.  Magistrala back-End SAS 12Gbps lub wydajniejsza.  Obsługa minimum 400 dysków SSD, SAS i NLSAS.  Pamięć cache macierzy musi być podtrzymywana ma wypadek zaniku zasilania przez okres minimum 7 dni lub zapisywana na trwały nośnik.  Musi posiadać wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). |
| **Pamięć cache** | Musi posiadać minimum 500GB pamięci macierzy pozwalającej na jednoczesne odczyty i zapisy, dostępnej jednocześnie dla wszystkich zasobów dyskowych macierzy, realizowanej z wykorzystaniem pamięci typu DDR i/lub dysków/pamięci Flash.  Zamawiający dopuszcza także macierz posiadającą minimum 128GB pamięci podręcznej pozwalającej na jednoczesne odczyty i zapisy, dostępnej jednocześnie dla wszystkich zasobów dyskowych macierzy, realizowanej z wykorzystaniem pamięci typu DDR. W tym przypadku dodatkowo wymagane jest dostarczenie dysków/pamięci Flash, które umożliwią rozbudowę pamięci podręcznej macierzy o dodatkowe minimum 1.92TB dostępne dla operacji odczytu. Jeśli do rozbudowy pamięci podręcznej z użyciem dysków/pamięci Flash niezbędna jest dodatkowa licencja, musi zostać ona dostarczona wraz z oferowaną macierzą. |
| **Porty** | Wyposażona w minimum 8 portów 25Gb/s~~,~~  Wyposażona w minimum 4 porty FC 16Gb/s wraz z wkładkami Single Mode,  Musi posiadać możliwość rozbudowy do co najmniej 16 portów 25Gb/s bez wymiany kontrolerów. |
| **Obsługa RAID** | Musi posiadać obsługę minimum RAID typu 10, 5 i 6 lub być wyposażona w technologie RAID z wykorzystaniem podwójnej i potrójnej parzystości. |
| **Dyski** | Musi posiadać zainstalowane minimum:  - 23 dyski 1.8TB SAS 12Gbps 10K RPM (identyczne jak w istniejącej macierzy dyskowej) |
| **Funkcjonalności** | Macierz musi zostać dostarczona z minimum następującym zestawem funkcjonalności dla całej pojemności macierzy:  Thin provisioning: możliwość udostępniania dla hostów większej przestrzeni, niż fizyczna przestrzeń dostępna w macierzy.  Tiering: możliwość migracji danych pomiędzy dyskami wykonanymi w różnych technologiach (możliwa migracja w jednej puli dyskowej pomiędzy co najmniej trzema typami dysków SSD, SAS i NLSAS).  Snapshoty: możliwość wykonywania snapshotów zgodnie z technologią Redirect-on-Write, w wypadku stosowanie innych technik wykonywania snapshotów, należy dostarczyć dodatkową pulę co najmniej 8 dysków SSD o pojemności co najmniej 1,6TB każdy oraz posiadające parametr DWPD na poziomie minimum 3.  Hot-Spare: obsługa dysków Hot Spare lub przestrzeni Hot Spare.  QoS: możliwość monitorowania wydajności zasobów dyskowych udostępnianych z macierzy.  Replikacja: musi umożliwiać co najmniej replikację asynchroniczną i synchroniczną dla danych blokowych i plikowych.  Obsługiwane protokoły minimum: FC (Fibre Channel), iSCSI, VMware VVOL 2.0, NFS 4.1 (Microsoft Windows 2019 Serwer), SMB 3.0.  Tryb pracy: możliwość połączenia z Hostami zarówno poprzez przełączniki jak również w trybie Direct Host Attach co najmniej dla protokołów iSCSI i FC.  Obsługiwana integracja z API rozwiązań wirtualizacyjnych conajmniej: VMware VAAI i VASA i Microsoft Hyper-V: ODX (Offloaded Data Transfer) i Offload Copy for File.  Licencje na wszystkie powyższe funkcjonalności muszą być dostarczone dla maksymalnej pojemności dostarczanej macierzy. |
| **Zasilanie i chłodzenie** | Musi być wyposażona w redundantne wentylatory.  Musi być wyposażona w redundantne zasilacze typu Hot-Swap. |
| **Oprogramowanie  do automatyzacji przełączania** | Macierz musi posiadać wsparcie dla oferowanego oprogramowania do automatyzacji przełączania, musi się znajdować na oficjalnych listach kompatybilności producenta zaoferowanego oprogramowania do automatyzacji przełączania. |
| **Certyfikaty** | ISO-9001 oraz ISO-14001. Deklaracja CE. |
| **Warunki gwarancji** | 60 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta oraz, że uszkodzone dyski w przypadku wymiany z powodu awarii w okresie obowiązywania gwarancji, pozostaną własnością Zamawiającego. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą. |

* + 1. **Półka dyskowa**

Wymagane jest dostarczenie 2 szt. półki dyskowej spełniającej poniżej opisane minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Kompatybilność** | Zamawiający posiada macierz dyskową DELL EMC Unity XT 380 – posiadająca następujące wyposażenie:  Dyski: 23x 1.8 TB SAS 10k, 2x 400 GB FLASH SSD  Porty komunikacyjne po stronie Hostów: 4x FC 16Gb/s, 8x 25 Gb/s  Magistrala back-End SAS 12Gbps lub wydajniejsza.  Zamawiający wymaga, aby oferowana półka dyskowa byłą kompatybilna z posiadaną macierzą. |
| **Obudowa** | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.  Musi posiadać minimum 25 wnęk na dyski 2,5”.  Magistrala back-End SAS 12Gbps lub wydajniejsza. |
| **Dyski** | Musi posiadać zainstalowane minimum:  - 10 dysków 1.2 TB SAS 12Gbps 10K RPM |
| **Warunki gwarancji** | 60 miesięcy gwarancji producenta realizowanej w miejscu instalacji sprzętu.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |

* + 1. **Macierz dyskowa - aktualizacja**

|  |  |
| --- | --- |
| **Kompatybilność** | Zamawiający posiada macierz dyskową DELL EMC Unity XT 380 s/n CRK00225006316 posiadająca następujące wyposażenie:  Dyski: 23x 1.8 TB SAS 10k, 2x 400 GB FLASH SSD  Porty komunikacyjne po stronie Hostów: 4x FC 16Gb/s, 8x 25 Gb/s  Magistrala back-End SAS 12Gbps lub wydajniejsza. |
| **Warunki gwarancji** | Zamawiający wymaga dla posiadanej macierzy dyskowej, wydłużenia okresu gwarancji producenta realizowanej w miejscu instalacji sprzętu, tak, aby okres i poziom tej gwarancji był zgodny z poziomem i okresem zakończenia gwarancji, dostarczanej w niniejszym postępowaniu nowej macierzy dyskowej.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |

## Oprogramowanie systemowe i narzędziowe

* + 1. **Licencje oprogramowania wirtualizacji klastra dziedzinowego oraz wirtualizacji stacji roboczych (klaster podstawowy i zapasowy)**

Wymagane jest dostarczenie 1 kpl. oprogramowania wirtualizacji.

Licencje muszą obejmować (w sumie 20 CPU):

• 4 sztuk serwerów wirtualizacji – każdy serwer po 2 CPU

• 6 sztuk serwerów dziedzinowych – udostępnionych przez Zamawiającego – każdy serwer po 2 CPU

• 2 sztuki serwerów centralnego zarządzania, każdy z serwerów zarządzania bez limitu liczby zarządzanych serwerów fizycznych,

• oprogramowanie do automatyzacji procesu przełączania dla 25 maszyn wirtualnych

Oprogramowanie musi posiadać następujące, wbudowane cechy:

|  |  |
| --- | --- |
| **Oprogramowanie wirtualizacji serwerów** | Oprogramowanie do wirtualizacji serwerów musi umożliwiać uruchomienie posiadanych przez Zamawiającego systemów stworzonych w formacie wirtualnych maszyn Vmware ESXi virtual harware version: 11, 13, 15, 17 i 19 |
|  | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. |
| Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB. |
| Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM. |
| Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. |
| Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. |
| Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB. |
| Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej. |
| Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. |
| Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS. |
| Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. |
| System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego 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 musi mieć możliwość konfiguracji do 4000 portów. |
| 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. |
| Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |
| 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). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM. |
| Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP. |
| Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. |
| Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych. |
| Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora. |
| Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej. |
| Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej. |
| Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej. |
| 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. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci. |
| Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej. |
| Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej. |
| Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory. |
| Oprogramowanie musi posiadać serwer do centralnego zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych:   1. globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych 2. wykonywanie automatycznych bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych. 3. widok całego systemu i zbioru maszyn wirtualnych. Mapy Infrastruktury. 4. możliwość monitorowania dostępności i wydajności maszyn wirtualnych 5. możliwość raportowania dostępności i wydajności maszyn wirtualnych 6. funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows 7. planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych 8. tworzenie obrazów maszyn wirtualnych 9. klonowanie maszyn wirtualnych 10. wykonywanie wielu kopii migawkowych (snapshoot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii |
| 1. Wymaga się dostarczenia opisanego oprogramowania z okresem wsparcia na 60 miesięcy. |
| **Oprogramowanie  do automatyzacji przełączania** | Licencje oprogramowania współpracujące z oprogramowaniem do wirtualizacji dla 25VM (maszyn wirtualnych), 5 lat wsparcia producenta.  Licencje wieczyste.  Opis funkcjonalności:   * + - * 1. Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych niezależnie od architektury DataCenter (Active-Active, Active-Pasive).         2. Rozwiązanie musi posiadać taką architekturę, aby umożliwiać wykonanie planu awaryjnego nawet w przypadku całkowitej niedostępności pojedynczego centrum danych         3. Rozwiązanie musi umożliwiać zapewnienie ochrony maszyn wirtualnych z dyskami wirtualnymi         4. Rozwiązanie musi być niezależne od producenta zastosowanego sprzętu fizycznego.         5. Rozwiązanie musi umożliwiać wykonywanie procedur przełączanie usług IT z ośrodka podstawowego do ośrodka zapasowego (fail-over) i z powrotem (fail-back) w ramach jednego narzędzia/konsoli.         6. Rozwiązanie musi umożliwiać wykonywanie tzw. planowanego przełączania pojedynczych maszyn wirtualnych lub grup wirtualnych maszyn do ośrodka zapasowego, polegające na wykonaniu scenariusza na który składają się automatycznie następujące po sobie kroki: poprawne zamkniecie wirtualnych maszyn po stronie centrum podstawowego, resynchronizacja replik danych, prezentacja replik danych po stronie odtworzeniowej, uruchomienie maszyn wirtualnych w ośrodku zapasowym.         7. Proces przełączania usług IT pomiędzy Centrami Przetwarzania Danych musi być automatyczny tzn. – nie wymagający interwencji administratora w żadnej warstwie infrastruktury – CPU, RAM, LAN, SAN.         8. Proces przełączania usług IT pomiędzy Centrami Przetwarzania Danych musi być uruchamiany w oparciu o decyzje administratora.         9. Rozwiązanie musi umożliwiać tworzenie planów przełączeniowych, konfigurowanie tych planów i przypisywanie do nich maszyn wirtualnych.         10. Rozwiązanie musi umożliwiać ochronę minimum 25 maszyn wirtualnych oraz posiadać 5 lat wsparcia. |

* + 1. **Licencje systemu operacyjnego serwera wirtualizacji**

1. Oprogramowanie musi posiadać następujące, wbudowane cechy:

|  |  |
| --- | --- |
| **Oprogramowanie systemu operacyjnego serwera** | Windows Server 2022 Datacenter, liczba licencji zgodna z oferowaną ilością rdzeni procesorów w serwerach wirtualizacji (4 szt.) lub systemy równoważne.  Zamawiający dopuszcza licencje typu OEM oraz ROK.  Opis równoważności:  Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i nielimitowanej ilości wirtualnych środowisk systemu operacyjnego serwerze za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy:  1. Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym  2. Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.  3. Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.  4. Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7. Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8. Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  - pozwalają na zmianę rozmiaru w czasie pracy systemu,  - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  - umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,  - umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10. Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11. Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12. Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13. Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14. Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15. Graficzny interfejs użytkownika.  16. Zlokalizowane w języku polskim, następujące elementy:  - menu,  - przeglądarka internetowa,  - pomoc,  - komunikaty systemowe.  17. Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  18. Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  19. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  20. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).  21. Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  • Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  - Zdalna dystrybucja oprogramowania na stacje robocze.  - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  • Dystrybucję certyfikatów poprzez http  • Konsolidację CA dla wielu lasów domeny,  - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.  - Szyfrowanie plików i folderów.  - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  - Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.  - Serwis udostępniania stron WWW.  - Wsparcie dla protokołu IP w wersji 6 (Ipv6),  - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla:  • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  • Obsługi ramek typu jumbo frames dla maszyn wirtualnych,  • Obsługi 4-KB sektorów dysków,  • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  - Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)  - Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  22. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).  23. Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  24. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  25. Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Licencje połączeniowe** | MS Windows 2022 DEV CAL lub równoważne – 350 szt.  Opis równoważności:  Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla 350 urządzeń.  Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej. |
| **Licencje połączeniowe pulpitu zdalnego** | MS Windows 2022 Remote Desktop Services DEV CAL lub równoważne – 500 szt.  Opis równoważności:  Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także zdalny dostęp do zasobów serwera dla 500 urządzeń.  Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej. |

* + 1. **Licencje systemu operacyjnego serwera backupu**

1. Oprogramowanie musi posiadać następujące, wbudowane cechy:

|  |  |
| --- | --- |
| **Oprogramowanie**  **systemu operacyjnego serwera** | Windows Server 2022 Standard, liczba licencji zgodna z oferowaną ilością rdzeni procesorów w serwerze backupu (1 szt.) - lub równoważne.  Zamawiającydopuszcza licencje typu OEM oraz ROK.  Opis równoważności:  Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch maszyn wirtualnych środowisk systemu operacyjnego serwerze za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy:  1. Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym  2. Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.  3. Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.  4. Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  5. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  6. Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  7. Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  8. Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  - pozwalają na zmianę rozmiaru w czasie pracy systemu,  - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  - umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,  - umożliwiają zdefiniowanie list kontroli dostępu (ACL).  10. Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  11. Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  12. Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  13. Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  14. Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  15. Graficzny interfejs użytkownika.  16. Zlokalizowane w języku polskim, następujące elementy:  - menu,  - przeglądarka internetowa,  - pomoc,  - komunikaty systemowe.  17. Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  18. Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  19. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  20. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).  21. Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  • Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  - Zdalna dystrybucja oprogramowania na stacje robocze.  - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  • Dystrybucję certyfikatów poprzez http  • Konsolidację CA dla wielu lasów domeny,  - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.  - Szyfrowanie plików i folderów.  - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  - Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.  - Serwis udostępniania stron WWW.  - Wsparcie dla protokołu IP w wersji 6 (Ipv6),  - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  - Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla:  • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  • Obsługi ramek typu jumbo frames dla maszyn wirtualnych,  • Obsługi 4-KB sektorów dysków,  • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  - Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)  - Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  22. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).  23. Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  24. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  25. Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |

* + 1. **Licencje systemu antywirusowego**

1. Oprogramowanie musi posiadać następujące, wbudowane cechy:

|  |  |
| --- | --- |
| **Oprogramowanie systemu antywirusowego** | Licencje muszą być kompatybilne z posiadanym przez Zamawiającego systemem ESET Protect Advanced On-Prem – licencja na okres 60 miesięcy lub system antywirusowy równoważny.  Liczba licencji: 360 sztuk.  Opis równoważności:  Oprogramowanie antywirusowe spełniające poniższe funkcjonalności:  **Ochrona stacji roboczych - Windows**   1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11 – Zamawiający dopuszcza rozwiązanie w ramach którego na podstawie otrzymanej licencji będzie upoważniony do zainstalowania poprzednich wersji otrzymanego oprogramowania wspierającego również systemy operacyjne Windows 7 i 8. 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim. 4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim. 6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.   **Ochrona antywirusowa i antyspyware**   1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 3. Wbudowana technologia do ochrony przed rootkitami. 4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. 8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość skanowania dysków sieciowych i dysków przenośnych. 12. Skanowanie plików spakowanych i skompresowanych. 13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 14. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. 18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 20. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 21. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 22. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 23. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 24. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 25. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. 27. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. 28. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. 29. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 30. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 31. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. 32. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. 33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 34. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. 36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 37. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. 38. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 39. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 40. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. 41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 43. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 44. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 45. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 46. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. 47. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 48. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. 49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 51. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 52. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. 53. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 54. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. 55. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 56. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 57. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. 58. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:     * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,     * tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,     * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,     * tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,     * tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 60. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 61. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 62. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 63. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 64. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 65. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa. 66. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. 67. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 68. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 69. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. 70. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 71. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 72. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 73. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 74. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. 75. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji. 76. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. 77. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń. 78. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. 79. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. 80. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. 81. Możliwość podejrzenia informacji o licencji, która znajduje się w programie. 82. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM. 83. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. 84. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 85. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. 86. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. 87. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 88. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. 89. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. 90. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. 91. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. 92. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 93. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. 94. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. 95. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. 96. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”. 97. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 98. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 99. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 100. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego. 101. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* 102. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet. 103. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.   **Ochrona przed spamem**   1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. 2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. 5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego. 6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. 7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam. 8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook. 9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana” 10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”. 11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.   **Zapora osobista (personal firewall)**   1. Zapora osobista ma pracować w jednym z czterech trybów:    * tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,    * tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,    * tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,    * tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 2. Program musi oceniać reguły zapory systemu Windows. 3. Możliwość tworzenia list sieci zaufanych. 4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. 5. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. 6. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. 7. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. 8. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet. 9. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. 10. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. 12. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 13. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. 14. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. 15. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci. 16. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:  * z aplikacją lokalną, którą administrator wskazuje z listy, * z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.   **Kontrola dostępu do stron internetowych**   1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych. 2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. 3. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 4. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 5. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. 6. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. 7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. 8. Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. 9. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.   **Bezpieczna przeglądarka**   1. Aplikacja musi być wyposażona w moduł bezpiecznej przeglądarki. 2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 3. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. 4. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. 5. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. 6. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. |

* + 1. **Licencje systemu backupu**

1. Oprogramowanie musi posiadać następujące, wbudowane cechy:

|  |  |
| --- | --- |
| **Oprogramowanie**  **systemu backupu** | Veeam Backup & Replication Community Edition (darmowa edycja) lub inne oprogramowanie backupowe umożliwiające wykonywanie backupu i jego odtworzenia wdrażanego środowiska.  Opis równoważności:   1. Oprogramowanie musi umożliwiać backup minimum 10 maszyn wirtualnych z dostarczanych 2 serwerów 2 procesorowych. 2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. 3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. 4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. 5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V. 6. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z serwerów plikowych opartych o Windows i Linux. 7. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. 8. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny i przyrostowy. 9. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. 10. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. 11. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. 12. 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. 13. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. 14. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora. 15. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli. 16. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing). 17. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre. 18. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. 19. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. 20. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:   1) Linux: ext2, ext3, ext4, ReiserFS, XFS,  2) Solaris ZFS, UFS,  3) Windows NTFS, FAT32, ReFS,   1. Oprogramowanie musi wspierać odtwarzanie wybranych obiektów i atrybutów Active Directory włączając hasło, obiekt użytkownika i komputera 2. Oprogramowanie musi wspierać odzyskiwanie elementów skrzynek pocztowych Microsoft Exchange 2010 i nowszych 3. Oprogramowanie musi wspierać odzyskiwanie plików baz danych Microsoft SQL 2005 i nowsze 4. Oprogramowanie musi wspierać odzyskiwanie elementów Microsoft Sharepoint 2010 i nowsze   Kompatybilność   * Zamawiający wymaga, aby licencja była kompatybilna z dostarczanym Serwerowym Systemem Operacyjnym SSO. |
|  |  |

## Usługi w zakresie infrastruktury serwerowej

* + 1. **Usługi – klaster wirtualizacyjny stacji roboczych**

Zamawiający wymaga wdrożenia zaoferowanych rozwiązań w trybie wysokiej dostępności. Wdrażany system będzie zlokalizowany w dwóch fizycznie oddzielnych lokalizacjach/ośrodkach przetwarzania danych Zamawiającego. W każdym z ośrodków przetwarzania Zamawiający dostarcza infrastrukturę dla uruchomienia dostarczanych urządzeń i oprogramowania (szafy RACK, zasilanie w tym również awaryjne wraz z listwami PDU zamontowanymi w szafach rack, chłodzenie/klimatyzację, system gaśniczy i kontroli dostępu). Zamawiający zapewnia również połączenie światłowodowe (single-mode) pomiędzy obydwoma ośrodkami obliczeniowymi. Systemy maja zostać skonfigurowane w architekturze wysokiej dostępności (również z wykorzystaniem posiadanej przez Zamawiającego macierzy dyskowej DELL EMC Unity XT 380)

Prace do wykonania:

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację, która składa się z nw. zakresów:

* Harmonogram Wdrożenia,
* Dokumentacja Analizy Przedwdrożeniowej (DAP) - Opracowanie projektu instalacji, wdrożenia i konfiguracji sprzętu i oprogramowania z zachowaniem najlepszych praktyk producentów dostarczanych rozwiązań z zachowaniem założonego poziomu wysokiej dostępności.

1. Instalacja, konfiguracja i wdrożenie dostarczonych urządzeń i oprogramowania, oraz integracja z systemami Zamawiającego:

* system bezpieczeństwa klasy UTM,
* sieć LAN rdzeń sieci, dostępowa i zarządzania,
* serwery, macierze dyskowe i system backupu,
* uruchomienie aplikacji klienckich w środowisku wirtualizacji stacji roboczych,
* system wirtualizacji w tym stacji roboczych,
* system replikacji i wysokiej dostępności,
* domena AD i usługi Microsoft, w tym DNS, DHCP, serwer certyfikatów, DFS, RADIUS,
* system antywirusowy wraz z ochroną środowiska wirtualnych desktopów,
* system backupu,
* opracowanie procedur bezpieczeństwa, utrzymania i disaster recovery.

1. Instalacja, konfiguracja i wdrożenie rozwiązania do wirtualizacji stacji roboczych:

* Instalacja elementów systemu,
* Wdrożenie i konfiguracja farmy serwerów obsługujących pulpity zdalne,
* Konfiguracja środowiska pulpitów zdalnych do pracy z aplikacji klienckimi i programami Zamawiającego
* Konfiguracja środowiska do pracy w dwóch ośrodkach obliczeniowych Zamawiającego,
* Konfiguracja dostępu do środowiska z wszystkich lokalizacji zdalnych Zamawiającego :

1. Szkoła Podstawowa nr 1, im. Jana Kochanowskiego, ul. 1-go Maja 11,
2. Szkoła Podstawowa nr 2, im. Jana Pawła II, ul. Ostrowiecka 134,
3. Szkoła Podstawowa nr 6, im. Obrońców Westerplatte, ul. Moniuszki 117,
4. Szkoła Podstawowa nr 9, im. Partyzantów Ziemi Kieleckiej, ul. Oświatowa 5,
5. Szkoła Podstawowa nr 10 z Oddziałami Integracyjnymi, im. Szarych Szeregów, al. Armii Krajowej 1,
6. Szkoła Podstawowa nr 11, im. majora Jana Piwnika „Ponurego”, ul. Leśna 2,
7. Szkoła Podstawowa nr 12, im. Mikołaja Kopernika, ul. Słoneczna 1a,
8. Szkoła Podstawowa nr 13, im. Kornela Makuszyńskiego, ul. Ignacego Prądzyńskiego 2
9. Przedszkole Miejskie nr 2 im. Kubusia Puchatka ul. Oświatowa 2,
10. Przedszkole Miejskie nr 6 ul. Świętej Barbary 4,
11. Przedszkole Miejskie nr 7 al. Armii Krajowej 6a,
12. Przedszkole Miejskie nr 10 Niezapominajka ul. Prądzyńskiego 2a,
13. Przedszkole Miejskie nr 11 z Oddziałami Integracyjnymi im. Misia Uszatka ul. Górna 13,
14. Przedszkole Miejskie nr 13 ul. Leśna 40,
15. Przedszkole Miejskie nr 14 im. Jana Brzechwy ul. Graniczna 10,
16. Przedszkole Miejskie nr 15 ul. Na Szlakowisku 7 b,
17. Centrum Usług Wspólnych, Radomska 45
18. Park Kultury, Radomska 21,
19. Centrum Usług Społecznych (CUS), ul. Majówka 21a,
20. Urząd Miejski,

a)ul. Radomska 45,

b)ul. Leśna 2 (budynek dawnego Gimnazjum nr 3)

1. Centrum Usług Społecznych (CUS), (Miejska Hala Targowa „Galeria Skałka)– Dom Senior Wigor „Manhattan”, Aleja Armii Krajowej 28
2. Miejska Biblioteka Publiczna i jej filie, ul. Kochanowskiego 5,

a)Filia nr 1 ul.Staszica 9

1. Filia nr 5 ul.Żeromskiego 8
2. Filia nr 6 ul.Staszica 9
3. Filia nr 7 ul.Radomska 21 (budynek parku kultury)
4. Filia nr 9 ul.Ostrowiecka 134 (budynek SP2)
5. Filia nr 10 ul.Prądzyńskiego 2 (budynek SP13)
6. Miejski Ośrodek Sportu i Rekreacji - Miejska Hala Sportowa, Al. Aleja Świętego Jana Pawła II 22
7. Miejski Ośrodek Sportu i Rekreacji -Kryta Pływalnia, ul. Szkolna 14b,
8. Centrum Usług Społecznych (CUS), Świetlica Środowiskowa ul. Widok 5
9. Centrum Usług Społecznych (CUS), Noclegownia ul .Radomska 53
10. Centrum Usług Społecznych (CUS), Środowiskowy Dom Samopomocy ul .Reja 10
11. Przeprowadzenie testów funkcjonalnych, obciążeniowych i disaster recover zakładających awarię naprzemiennie obydwu ośrodków obliczeniowych.
12. Przeprowadzenie testów akceptacyjnych.
13. Przygotowanie dokumentacji powykonawczej.
14. Świadczenie pomocy technicznej w okresie 5 lat od zakończenia wdrożenia systemów w wymiarze minimum 480 godzin on-line i minimum dodatkowych 160 godzin on-site.

Zapewnienie poza wskazanymi powyżej godzinami świadczenia pomocy technicznej, przynajmniej jeden raz na każde 12 miesięcy kalendarzowych, wykonanie pełnej aktualizacji całego wdrożonego środowiska do najnowszych wspieranych wersji przez producentów rozwiązań, prace wykonywane poza godzinami pracy Zamawiającego.

* + 1. **Usługi – klaster dziedzinowy**

Zamawiający udostępni na potrzeby projektu dla budowy klastra dziedzinowego, sprzęt w postaci sześciu serwerów z procesorami w architekturze Intel Xeon wraz z licencjami serwerowych systemów operacyjnych (Zamawiający wymaga wdrożenia udostępnionego sprzętu w trybie wysokiej dostępności). Powyższe serwery oraz licencje systemów operacyjnych nie są przedmiotem dostawy w tym postepowaniu.

Zamawiający wymaga wdrożenia zaoferowanych rozwiązań w trybie wysokiej dostępności. Wdrażany system będzie zlokalizowany w dwóch fizycznie oddzielnych lokalizacjach/ośrodkach przetwarzania danych Zamawiającego.

W każdym z ośrodków przetwarzania Zamawiający dostarcza infrastrukturę dla uruchomienia dostarczanych urządzeń i oprogramowania (szafy RACK, zasilanie w tym również awaryjne wraz z listwami PDU zamontowanymi w szafach rack, chłodzenie/klimatyzację, system gaśniczy i kontroli dostępu). Zamawiający zapewnia również połączenie światłowodowe pomiędzy obydwoma ośrodkami obliczeniowymi. Systemy maja zostać skonfigurowane w architekturze wysokiej dostępności (również z wykorzystaniem posiadanej przez Zamawiającego macierzy dyskowej DELL EMC Unity XT 380).

Wykonawca dokona niezbędnych uzgodnień podczas wdrożenia systemów backupowych i odtworzeniowych z rozwiązaniami dostarczonymi przez Wykonawcę oprogramowywania dziedzinowego.

Prace do wykonania:

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację, która składa się z nw. zakresów:

* Harmonogram Wdrożenia,
* Dokumentacja Analizy Przedwdrożeniowej (DAP) - Opracowanie projektu instalacji, wdrożenia i konfiguracji sprzętu i oprogramowania z zachowaniem najlepszych praktyk producentów dostarczanych rozwiązań z zachowaniem założonego poziomu wysokiej dostępności.

1. Instalacja, konfiguracja i wdrożenie dostarczonych urządzeń i oprogramowania oraz integracja z systemami Zamawiającego:

* system replikacji i wysokiej dostępności,
* system antywirusowy,
* system backupu,
* opracowanie procedur bezpieczeństwa, utrzymania i disaster recovery.

1. Przeprowadzenie testów funkcjonalnych, obciążeniowych i disaster recover zakładających awarię naprzemiennie obydwu ośrodków obliczeniowych.
2. Przeprowadzenie testów akceptacyjnych.
3. Przygotowanie dokumentacji powykonawczej.
4. Świadczenie pomocy technicznej w okresie 5 lat od zakończenia wdrożenia systemów w wymiarze minimum 120 godzin on-line i minimum dodatkowych 40 godzin on-site.
5. Zapewnienie poza wskazanymi powyżej godzinami świadczenia pomocy technicznej, przynajmniej jeden raz na każde 12 miesięcy kalendarzowych, wykonanie pełnej aktualizacji całego wdrożonego środowiska do najnowszych wspieranych wersji przez producentów rozwiązań, prace wykonywane poza godzinami pracy Zamawiającego.
6. Zamawiający oczekuje migracji środowiska dziedzinowego (do 25 maszyn wirtualnych)
   * 1. **Instruktaże/ warsztaty**

Wykonawca musi przeprowadzić szkolenie o następujących minimalnych wymaganiach:

Warsztat oraz instruktaż 1:

• warsztat dla trzech pracowników Zamawiającego,

• warsztat z wdrożonego rozwiązania wirtualizacji stacji roboczych,

• czas trwania minimum 2 dni (każdy dzień minimum 8 godzin lekcyjnych każda po 45 minut),

• warsztat przeprowadzone w języku polskim, dostarczone materiały w języku polskim,

• część praktyczna (warsztaty i ćwiczenie) musi stanowić maksimum 50% czasu,

* warsztaty należało będzie przeprowadzić po wcześniejszym ustaleniu z Zamawiającym, termin oraz miejsce warsztatów zostanie ustalone na etapie wdrożeniowym,
* instruktaże przeprowadzone zostaną dla pięciu pracowników Zamawiającego,

na dostarczonej przez Wykonawcę w ramach zamówienia infrastrukturze, instruktaż przeprowadzony będzie w siedzibie Zamawiającego (1 dzien).

Warsztat oraz instruktaż 2:

• warsztat dla trzech pracowników Zamawiającego,

• warsztat z wdrożonego rozwiązania macierzy dyskowych i serwerów,

• czas trwania minimum 2 dni (każdy dzień minimum 8 godzin lekcyjnych każda po 45 minut),

• warsztat przeprowadzone w języku polskim, dostarczone materiały w języku polskim,

• część praktyczna (warsztaty i ćwiczenie) musi stanowić maksimum 50% czasu,

* warsztaty należało będzie przeprowadzić po wcześniejszym ustaleniu z Zamawiającym, termin oraz miejsce warsztatów zostanie ustalone na etapie wdrożeniowym,
* instruktaże przeprowadzone zostaną dla pięciu pracowników Zamawiającego,

na dostarczonej przez Wykonawcę w ramach zamówienia infrastrukturze, instruktaż przeprowadzony będzie w siedzibie Zamawiającego (1 dzien).

Warsztat oraz instruktaż 3:

• warsztat dla trzech pracowników Zamawiającego,

• warsztat z wdrożonego rozwiązania wirtualizacji serwerów,

• czas trwania minimum 2 dni (każdy dzień minimum 8 godzin lekcyjnych każda po 45 minut),

• warsztat przeprowadzone w języku polskim, dostarczone materiały w języku polskim,

• część praktyczna (warsztaty i ćwiczenie) musi stanowić maksimum 50% czasu,

* warsztaty należało będzie przeprowadzić po wcześniejszym ustaleniu z Zamawiającym, termin oraz miejsce warsztatów zostanie ustalone na etapie wdrożeniowym,
* instruktaże przeprowadzone zostaną dla pięciu pracowników Zamawiającego,

na dostarczonej przez Wykonawcę w ramach zamówienia infrastrukturze, instruktaż przeprowadzony będzie w siedzibie Zamawiającego (1 dzien).

# Gwarancja

## Okres gwarancji

1. Wykonawca w ramach realizacji przedmiotu zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) tj.:
   1. **Infrastruktura serwerowa w zakresie:**

|  |  |  |
| --- | --- | --- |
| **Poz. OPZ** | **Opis** | **Okres gwarancji (minimalny)\*** |
| **Rozdział II.1** | **Infrastruktura serwerowa** |  |
| II.1.1 | Serwer wirtualizacyjny produkcyjny | 60 miesięcy |
| II.1.2 | Serwer backupu | 60 miesięcy |
| II.1.3 | Macierz dyskowa | 60 miesięcy |
| II.1.4 | Półka dyskowa | 60 miesięcy |
| II.1.5 | Macierz dyskowa - aktualizacja | 60 miesięcy |

* 1. **Oprogramowanie systemowe i narzędziowe w zakresie:**

|  |  |  |
| --- | --- | --- |
| **Poz. OPZ** | **Opis** | **Okres gwarancji (minimalny)\*** |
| **Rozdział II.2** | **Oprogramowanie systemowe i narzędziowe** |  |
| II.2.1 | Licencje oprogramowania wirtualizacji klastra dziedzinowego oraz wirtualizacji stacji roboczych (klaster podstawowy i zapasowy) | 60 miesięcy |
| II.2.2 | Licencje systemu operacyjnego serwera wirtualizacji | --------------- |
| II.2.3 | Licencje systemu operacyjnego serwera backupu | --------------- |
| II.2.4 | Licencje systemu antywirusowego | 60 miesięcy |
| II.2.5 | Licencje systemu backupu | 60 miesięcy |

1. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem Protokołu Końcowego bez uwag przez Zamawiającego.
2. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta.

## Reżimy realizacji usług serwisowych

W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia (dotyczy infrastruktury sieci teleinformatycznej, infrastruktury serwerowej oraz sieciowej) rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami, jak poniżej:

1. **Awaria -** Kategoria Wady w Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której Oprogramowanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia.
2. **Usterka -** Należy przez to rozumieć kategorię Wady w Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.

**Tabela 1. Gwarancja dla Infrastruktury serwerowej:**

1. Serwery wirtualizacji,
2. Serwer backupu,
3. Macierze dyskowe,
4. Półki dyskowe

| **KWALIFIKACJA ZGŁOSZENIA WADY** | **OKRES DOSTĘPNOŚCI WYKONAWCY** | **ROZWIĄZANIE  ZASTĘPCZE** | **CZAS REAKCJI WYKONAWCY** | **CZAS NAPRAWY** |
| --- | --- | --- | --- | --- |
| AWARIA | 24/7/365 | niezwłocznie, nie później niż 12 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia | niezwłocznie,  nie później niż 4 dni robocze od czasu zgłoszenia |
| USTERKA | 24/7/365 | niezwłocznie, nie później niż 3 dni od czasu przyjęcia zgłoszenia | niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia | niezwłocznie, nie  później niż 10 dni roboczych od czasu zgłoszenia |

1. Dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną.
2. Czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 1).
3. W przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego.
4. Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy.

## Pozostałe ustalenia

1. System Zgłoszeń, który zostanie udostępniony przez Wykonawcę, ma dodatkowo pozwalać na prowadzenie rejestru kontaktów z Zamawiającym obejmującego w szczególności wykonane czynności gwarancyjne, ewidencję wszystkich zgłoszeń gwarancyjnych, opis zmian w konfiguracji Oprogramowania; prowadzenie rejestru zgłoszeń jest obowiązkiem Wykonawcy.
2. Gwarancja i serwis na urządzenia muszą być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji.

Uwaga:

W przypadku zapisu terminu, jako:

1. Dzień Roboczy - wszystkie dni z pominięciem sobót, niedziel i świąt ustawowo wolnych od pracy.
2. Godziny Robocze należy rozumieć godziny od 7.30 do 15.30 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.