(Znak postępowania: GKI.271.24.2022)

**Załącznik nr 1 do SWZ. Szczegółowy opis przedmiotu zamówienia, wersja z dnia 03.10.2022**

Dotyczy zamówienia publicznego pn. Dostawa sprzętu komputerowego z oprogramowaniem dla Gminy Sanok w ramach projektu „Cyfrowa Gmina”

# Część 1. Dostawa stacji roboczych, laptopów i oprogramowania

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Stacje robocze (komputery stacjonarne z systemem operacyjnym i monitorem) | 30 |
| Laptopy z systemem operacyjnym | 15 |
| Pakiety oprogramowania biurowego | 30 |

Kody CPV:

* + - * 30213000-5 Komputery osobiste
      * 30213100-6 Komputery przenośne
      * 30231300-0 Monitory ekranowe
      * 48000000-8 Pakiety oprogramowania i systemy informatyczne
      * 48422000-2 Zestawy pakietów oprogramowania
      * 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
      * 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

## Stacje robocze (komputery stacjonarne z systemem operacyjnym i monitorem)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer stacjonarny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. | TAK / NIE |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach stacjonarnych, uzyskujący wynik co najmniej 12 000 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK / NIE  Procesor: ……………………………………………………………..  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 64 GB, co najmniej jeden wolny slot na moduły pamięci. | TAK / NIE |
| Pamięć masowa | Co najmniej 512 GB NVMe SSD M.2.  Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”. | TAK / NIE |
| Karta graficzna | Zintegrowana lub dedykowana karta graficzna. | TAK / NIE |
| Wyposażenie multimedialne | Karta dźwiękowa co najmniej dwukanałowa zintegrowana z płytą główną. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie typu combo (wspólny port słuchawkowo – mikrofonowy)~~, na tylnym panelu co najmniej port audio line-out~~. | TAK / NIE |
| Obudowa | Typu small form factor (suma wymiarów obudowy nieprzekraczająca 700 mm).  Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi. Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie i wpisanym na stałe w BIOS. | TAK / NIE |
| Zasilacz | Zasilacz o mocy nieprzekraczającej **240W** pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności co najmniej 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności co najmniej 80% przy obciążeniu zasilacza na poziomie 100%. | TAK / NIE |
| Bezpieczeństwo | Układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu musi prowadzić do uszkodzenia całej płyty głównej. | TAK / NIE |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. | TAK / NIE |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. | TAK / NIE |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | TAK / NIE |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat);  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: ……………………………………………………………………..  (należy wpisać producenta, nazwę i wersję systemu) |
| Wymagania dodatkowe | Wbudowane porty – co najmniej:  2 szt. DisplayPort lub 2 szt. HDMI lub 1 szt. DisplayPort i 1 szt. HDMI  Co najmniej 6 portów USB, w tym co najmniej 4 porty USB 3.x typu A i co najmniej 1 port USB 3.x typu C.  Co najmniej 2 porty USB 3.x spośród ww. muszą być umieszczone na przednim panelu obudowy.  Port audio typu combo (słuchawki/mikrofon) na przednim panelu obudowy.  ~~Port audio-out na tylnym panelu obudowy.~~  Port RJ – 45.  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich ww. portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika).  Klawiatura USB w układzie polski programisty.  Mysz USB z rolką (scroll).  Nagrywarka DVD +/-RW o prędkości co najmniej 8x.  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. | TAK / NIE |
| Ergonomia | Głośność komputera mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego nie może przekraczać **28** dB. ~~Do oferty należy załączyć dokument potwierdzający spełnienie wymagania sporządzony przez laboratorium akredytowane przez Polskie Centrum Akredytacji lub jako dokument równoważny oświadczenie producenta zestawu komputerowego dotyczące głośności tej jednostki.~~ | TAK / NIE |
| Monitor | Ekran o przekątnej co najmniej 23,8” z powłoką antyrefleksyjną.  Rozdzielczość natywna full HD (1080p) 1920 x 1080.  Jasność: co najmniej 250 cd/m². Kontrast: co najmniej 1000:1.  Kąty widzenia: co najmniej 178/178.  Wbudowane głośniki stereo.  Wbudowane porty: co najmniej HDMI, VGA, DisplayPort.  Wymagany kabel umożliwiający podłączenie do komputera przez porty HDMI lub DisplayPort. | TAK / NIE |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty komputera i monitor. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii ~~oraz samodzielne zamawianie zamiennych komponentów~~.  Możliwość sprawdzenia kompletnych danych o urządzeniu na ~~jednej~~ witrynie internetowej prowadzonej przez producenta (**dla komputera i monitora:** rodzaj gwarancji, data wygaśnięcia gwarancji~~,~~ **dla komputera:** automatyczna identyfikacja komputera, konfiguracja fabryczna, ~~konfiguracja bieżąca,~~ ~~data produkcji komputera~~, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK / NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego komputera:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Laptopy z systemem operacyjnym

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer mobilny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. | TAK / NIE |
| Ekran | Przekątna 15,6”, rozdzielczość co najmniej full HD (1920 x 1080), powłoka przeciwodblaskowa, jasność co najmniej 250 nitów, kontrast co najmniej 700:1. | TAK / NIE |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach przenośnych, uzyskujący wynik co najmniej 9 500 punktów w teście PassMark - CPU Mark według wyników procesorów publikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK / NIE  Procesor: ……………………………………………………………..  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 32 GB, co najmniej jeden wolny slot na moduły pamięci. | TAK / NIE |
| Pamięć masowa | Co najmniej 256GB NVMe SSD M.2. | TAK / NIE |
| Karta graficzna | Karta graficzna zintegrowana lub dedykowana. | TAK / NIE |
| Karta sieciowa | Zintegrowana, 10/100/1000 (RJ-45) dostępna bezpośrednio z obudowy bez konieczności używania dodatkowych adapterów. | TAK / NIE |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo.  Port audio typu combo (wspólne złącze obsługujące słuchawki i mikrofon).  Wbudowana kamera co najmniej 720p z mechaniczną przysłoną.  Czytnik kart czytający co najmniej karty micro SD. | TAK / NIE |
| Łączność bezprzewodowa | Wi-Fi generacji co najmniej 6  Bluetooth standardu co najmniej 5.1 | TAK / NIE |
| Bateria i zasilanie | Bateria co najmniej 45 Whr, umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.  Zasilacz dedykowany przez producenta. | TAK / NIE |
| Waga | Nie więcej niż 2 kg z baterią. | TAK / NIE |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. | TAK / NIE |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. | TAK / NIE |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. | TAK / NIE |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu musi powodować uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.  Czytnik linii papilarnych. | TAK / NIE |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat);  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: ……………………………………………………………………..  (należy wpisać producenta, nazwę i wersję systemu) |
| Klawiatura | Klawiatura z wydzieloną częścią numeryczną, podświetlana.  Touchpad z dwoma przyciskami. | TAK / NIE |
| Porty i złącza | Wbudowane porty i złącza – co najmniej:  1 szt. HDMI,  1 szt. RJ-45,  3 szt. USB (w tym co najmniej 1 szt. USB 3.x i 1 szt. USB 3.x z zasilaniem),  1 szt. USB 3.x typu C z zasilaniem,  port zasilania (nie zajmujący portu USB typ C),  złącze linki zabezpieczającej. | TAK / NIE |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii ~~oraz samodzielne zamawianie zamiennych komponentów~~.  Możliwość sprawdzenia kompletnych danych o urządzeniu na ~~jednej~~ witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, ~~konfiguracja bieżąca,~~ rodzaj gwarancji, data wygaśnięcia gwarancji, ~~data produkcji komputera,~~ aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK / NIE |
|  | Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Pakiety oprogramowania biurowego

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane oprogramowanie – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Zawartość pakietu | Pakiet musi zawierać:   * edytor tekstów, * arkusz kalkulacyjny, * narzędzie do przygotowania i prowadzenia prezentacji, * narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). | TAK / NIE |
| Wymagania ogólne dla pakietu | Wymagana pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.  Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach co najmniej od 8 do 15 – cena połączenia nie większa niż cena połączenia lokalnego.  Wymagany publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.  Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).  Wymagane dostarczenie licencji odpowiedniej dla jednostek samorządu terytorialnego.  Licencja musi obejmować najnowszą wersję pakietu dostępną na dzień składania oferty. | TAK / NIE |
| Edytor teksu | Edytor tekstu musi umożliwiać:   * Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. * Wstawianie oraz formatowanie tabel. * Wstawianie oraz formatowanie obiektów graficznych. * Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). * Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. * Automatyczne tworzenie spisów treści. * Formatowanie nagłówków i stopek stron. * Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Określenie układu strony (pionowa/pozioma). * Wydruk dokumentów. * Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. * Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. | TAK / NIE |
| Arkusz kalkulacyjny | Arkusz kalkulacyjny musi umożliwiać:   * Tworzenie raportów tabelarycznych. * Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. * Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. * Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). * Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. * Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. * Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. * Wyszukiwanie i zamianę danych. * Wykonywanie analiz danych przy użyciu formatowania warunkowego. * Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Formatowanie czasu, daty i wartości finansowych z polskim formatem. * Zapis wielu arkuszy kalkulacyjnych w jednym pliku. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. | TAK / NIE |
| Narzędzie do przygotowywania i prowadzenia prezentacji | Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:   * Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego. * Drukowanie w formacie umożliwiającym robienie notatek. * Zapisanie jako prezentacja tylko do odczytu. * Nagrywanie narracji i dołączanie jej do prezentacji. * Opatrywanie slajdów notatkami dla prezentera. * Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. * Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. * Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. * Możliwość tworzenia animacji obiektów i całych slajdów. * Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. | TAK / NIE |
| Narzędzie do zarządzania informacją prywatną | Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:   * Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. * Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. * Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. * Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. * Automatyczne grupowanie poczty o tym samym tytule. * Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. * Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. * Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. * Zarządzanie kalendarzem. * Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. * Przeglądanie kalendarza innych użytkowników. * Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. * Zarządzanie listą zadań. * Zlecanie zadań innym użytkownikom. * Zarządzanie listą kontaktów. * Udostępnianie listy kontaktów innym użytkownikom. * Przeglądanie listy kontaktów innych użytkowników. * Możliwość przesyłania kontaktów innym użytkowników. | TAK / NIE |

# Część 2. Dostawa sprzętu serwerowego i sieciowego z oprogramowaniem i usługami wdrożeniowymi

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Serwery z systemami operacyjnymi, oprogramowaniem do wirtualizacji i oprogramowaniem bazodanowym | 2 |
| Macierz dyskowa | 1 |
| Urządzenie NAS z oprogramowaniem do tworzenia kopii zapasowych (backup) | 1 |
| Przełączniki sieciowe | 2 |
| Oprogramowanie do nadzoru nad siecią LAN | 1 |
| Usługi wdrożeniowe | 1 |

Kody CPV:

* + - * 48820000-2 Serwery
      * 30233000-1 Urządzenia do przechowywania i odczytu danych
      * 32420000-3 Urządzenia sieciowe
      * 48000000-8 Pakiety oprogramowania i systemy informatyczne
      * 48422000-2 Zestawy pakietów oprogramowania
      * 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
      * 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

## Serwery z systemami operacyjnymi, oprogramowaniem do wirtualizacji i oprogramowaniem bazodanowym

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug,z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli . | TAK / NIE |
| Procesor | Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem uzyskujące w układzie dwuprocesorowym wynik co najmniej 34 000 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK/NIE  Procesor: …………………………………………………………….  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 256 GB DDR4 registered. Płyta główna musi obsługiwać do 2 TB pamięci RAM DDR4 lub więcej. | TAK / NIE |
| Grafika | Zintegrowana karta graficzna ze złączem VGA. | TAK / NIE |
| Sieć | Co najmniej: 4x 1Gbit Base-T oraz 2x 10 Gbit SFP+. | TAK / NIE |
| Dyski twarde | Zainstalowane 2 szt. dysków SSD SATA o pojemności co najmniej 240GB każdy, skonfigurowane w RAID-1 na sprzętowym kontrolerze ze wsparciem dla oferowanego systemu wirtualizacji | TAK / NIE |
| Kontrolery dyskowe | Zainstalowany kontroler SAS HBA posiadający 2 porty zewnętrzne umożliwiające podłączenie macierzy będącej przedmiotem zamówienia. | TAK / NIE |
| Porty | Co najmniej 3 zewnętrzne porty USB 3, w tym co najmniej 1 port na panelu przednim.  Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera. | TAK / NIE |
| Wentylacja | Redundantne wentylatory hotplug. | TAK / NIE |
| Zasilanie | Redundantne zasilacze hotplug o sprawności co najmniej 90% o mocy co najmniej 800 W każdy. | TAK / NIE |
| Diagnostyka | Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń, procesory  pamięć RAM, status karty zrządzającej serwera  wentylatory, zasilacze. System przewidywania / rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym). | TAK / NIE |
| Zarządzanie | Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, posiadający dedykowany port RJ-45 GbE umożliwiający co najmniej:   * + zdalne zarządzanie przez przeglądarkę,   + zdalny restart serwera,   + szyfrowane połączenie (TLS, SSL),   + przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),   + możliwość przejęcia konsoli tekstowej,   + obsługę protokołu LDAP,   + zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,   + zarządzanie alarmami (zdarzenia poprzez SNMP),   + możliwość backupu i odtworzenia ustawień BIOS serwera oraz ustawień karty zarządzającej,   + możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN,   + możliwość konfiguracji i wykonania aktualizacji BIOS, firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej,   + oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna). | TAK / NIE |
| Bezpieczeństwo | * Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych. * Moduł TPM 2.0. | TAK / NIE |
| Oprogramowanie – system wirtualizacji | Z serwerami należy dostarczyć pakiet oprogramowania przeznaczonego do wirtualizacji serwerów. Oprogramowanie do wirtualizacji serwerów będzie przeznaczone na cele utworzenia klastra wirtualizacyjnego składającego się z serwerów będących przedmiotem zamówienia.  Oprogramowanie musi posiadać następujące cechy i funkcjonalności:   1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi umożliwiać obsługę i wykorzystanie procesorów fizycznych wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. 6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows Server 2008, Windows Server 2012, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X. 13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 15. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. 16. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. 17. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 18. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 19. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 20. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. 21. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 22. 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. 23. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). | TAK / NIE  Oprogramowanie – system wirtualizacji: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Oprogramowanie bazodanowe | Z serwerami należy dostarczyć licencje na oprogramowanie bazodanowe.  Oprogramowanie bazodanowe (OBD) musi spełniać następujące wymagania poprzez wbudowane mechanizmy:   1. Możliwość wykorzystania OBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. 2. Zintegrowane narzędzia graficzne do zarządzania systemem – OBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania. 3. Zarządzanie serwerem za pomocą skryptów - OBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem. 4. Dedykowana sesja administracyjna - OBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 5. Możliwość automatycznej aktualizacji systemu - OBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania). 6. OBD musi umożliwiać tworzenie klastrów niezawodnościowych. 7. Wysoka dostępność - OBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:  * bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam OBD), * niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), * klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,  1. Kompresja kopii zapasowych - OBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha OBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych. 2. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych. 3. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory. 4. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - OBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. 5. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - OBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:  * odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system), * wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur), * para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).  1. Zarządzanie pustymi wartościami w bazie danych - OBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci. 2. Definiowanie nowych typów danych - OBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji. 3. Wsparcie dla technologii XML - OBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:  * udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli, * udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD, * udostępniać język zapytań do struktur XML, * udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML), * udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.  1. Wsparcie dla danych przestrzennych - OBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:  * zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów, * oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp., * obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu OBD, * typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).  1. Możliwość tworzenia funkcji i procedur w innych językach programowania - OBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego OBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania. 2. Możliwość tworzenia rekursywnych zapytań do bazy danych - OBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny. 3. Obsługa błędów w kodzie zapytań - język zapytań i procedur w OBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania. 4. Raportowanie zależności między obiektami - OBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych. 5. Mechanizm zamrażania planów wykonania zapytań do bazy danych - OBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji OBD, wprowadzeniu zmian sprzętowych serwera. 6. System transformacji danych - OBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:  * mechanizm debuggowania tworzonego rozwiązania, * mechanizm stawiania „pułapek” (breakpoints), * mechanizm logowania do pliku wykonywanych przez transformację operacji, * możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu), * możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo) * mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli), * mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach), * mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego, * mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.  1. Wbudowany system analityczny - OBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina. 2. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail). 3. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki). 4. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych. 5. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta). 6. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli. 7. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - OBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. 8. System raportowania - OBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:  * raporty parametryzowane, * cache raportów (generacja raportów bez dostępu do źródła danych), * cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów), * współdzielenie predefiniowanych zapytań do źródeł danych, * wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File), * możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport, * możliwość wizualizacji wskaźników KPI, * możliwość wizualizacji danych w postaci obiektów sparkline.  1. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services). 2. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach. 3. OBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów. 4. OBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja). 5. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT. 6. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache’u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD. 7. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań. 8. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).   Licencje dostarczone z obydwoma serwerami muszą łącznie umożliwiać eksploatację oprogramowania bez ograniczeń czasowych na co najmniej 4 rdzeniach procesora. | TAK / NIE  Oprogramowanie bazodanowe: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję oprogramowania) |
| System operacyjny | System operacyjny spełniający nw. wymagania minimalne:   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. 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. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. 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. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:        1. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,        2. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,        3. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.        4. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych.     3. Zdalna dystrybucja oprogramowania na stacje robocze.     4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej     5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:        1. Dystrybucję certyfikatów poprzez http        2. Konsolidację CA dla wielu lasów domeny,        3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,        4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     6. Szyfrowanie plików i folderów.     7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).     8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.     9. Serwis udostępniania stron WWW.     10. Wsparcie dla protokołu IP w wersji 6 (IPv6),     11. Wsparcie dla algorytmów Suite B (RFC 4869),     12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,     13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. 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 mają zapewnić wsparcie dla:         1. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,         2. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.         3. Obsługi 4-KB sektorów dysków         4. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra         5. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.         6. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31. Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.   Zaoferowane wraz z serwerami licencje na system operacyjny:   1. muszą obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 2. łącznie muszą uprawniać do zainstalowania tego systemu na co najmniej czterech serwerach wirtualnych w klastrze wirtualizacyjnym składającym się z dwóch serwerów fizycznych będących przedmiotem zamówienia, 3. łącznie muszą obejmować licencje dostępowe dla 70 użytkowników.   Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty serwera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta.  W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez infolinię lub portal producenta. | TAK / NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Macierz dyskowa

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa, możliwości rozbudowy macierzy | 1. System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maksymalnie 2U w tej szafie. 2. Obudowa pojedynczego modułu rozwiązania – półka dyskowa, moduł kontrolerów -musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia, umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy. 3. Macierz musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy. 4. Macierz nie może zawierać elementów typu bateria/akumulator wymagających jakiegokolwiek reżimu obsługowego: wymiana, przełączanie, ładowanie (np. nie dopuszcza się podtrzymania bateryjnego cache kontrolerów itp.). 5. Rozbudowa o dodatkowe moduły dyskowe (półki dyskowe) dla obsługiwanych dysków musi odbywać się wyłącznie poprzez zakup takich modułów tj. bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy. 6. Połączenia pomiędzy półkami dyskowymi muszą zapewniać brak pojedynczego punktu awarii. | TAK / NIE |
| Pojemność | 1. System musi umożliwiać instalację dysków wykonanych w technologii hot-plug i wyposażonych w podwójny interfejs SAS. 2. Macierz musi umożliwiać obsługę co najmniej 8 dysków SSD. 3. Zainstalowane 6 dysków SSD-SAS 960GB oraz 6 dysków NL-SAS 4TB. | TAK / NIE |
| Kontrolery | 1. System musi obsługiwać 2 kontrolery pracujące w układzie nadmiarowym typu active-active i bez konieczności stosowania zewnętrznych połączeń kablowych pomiędzy nimi, z minimum 8GB pamięci podręcznej w każdym kontrolerze, wymaga się dostarczenia minimum 2 kontrolerów. 2. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik. 3. Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia. 4. Macierz musi pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach nawet w przypadku konfiguracji z jednym kontrolerem RAID. 5. W układzie z zainstalowanymi dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror. 6. Każdy z kontrolerów RAID musi posiadać dedykowane min. 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością 1 Gb/s - dla zdalnej i lokalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. | TAK / NIE |
| Interfejsy | Minimum 2 porty iSCSI 10G na każdy kontroler macierzy do podłączenia serwerów. | TAK / NIE |
| Poziomy RAID | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1,1+0, 5, 5+0, 6. | TAK / NIE |
| Wspierane dyski | Oferowany model macierzy musi wspierać dyski:   1. dyski SAS wykonane w technologii hot-plug, 2. dyski NL-SAS (NearLine SAS) wykonane w technologii hot-plug, 3. dyski SSD SAS wykonane w technologii hot-plug, 4. interfejsy obsługiwanych dysków muszą być wyposażone w minimum 2 porty pracujące w reżimie full-duplex (jednoczesna transmisję danych przez dwa porty), 5. macierz musi wspierać mieszaną konfigurację dysków SSD, SAS i NearLine SAS w obrębie pojedynczego modułu obudowy, 6. macierz musi wspierać mechanizm automatycznej przedawaryjnej migracji zapisów i składowanych danych na dysk zapasowy. 7. macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych w trybie ręcznym i automatycznym z wykorzystaniem mechanizmu typu ‘time scheduler’ czyli w zadanym i/lub powtarzalnym oknie czasowym. 8. macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach:   - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID  hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID.   1. Macierz musi pozwalać na skonfigurowanie dowolnego dysku hot-plug dostarczonego w rozwiązaniu do roli dysku zapasowego jak w pkt.7 2. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. BackLessCopy) |  |
| Oprogramowanie, funkcjonalności | 1) Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na minimum 1024 kopie migawkowych.  2) Macierz musi wspierać Microsoft Volume ShadowCopy Services (VSS).  3) Macierz musi umożliwiać zdefiniowanie min. 1024 woluminów (LUN).  4) Macierz musi umożliwiać podłączenie logiczne z serwerami i stacjami poprzez minimum 4 ścieżki.  5) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek dla podłączonych stacji/serwerów.  6) Macierz musi umożliwiać rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD.  7) Oferowany model macierzy musi obsługiwać mechanizmy Thin Provisioning (przy zainstalowanych 2 kontrolerach) czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy – wymagana jest obsługa minimum 64 pól ThinProvisioning w rozwiązaniu.  8) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji:  - zmiana rozmiaru woluminu,  - zmiana poziomu RAID,  - zmiana technologii dysków dla danej grupy RAID,  - dodawanie nowych dysków do istniejącej grupy dyskowej,  9) Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server, SuSE Linux, RedHat Linux, Oracle Linux, Oracle VM, HP-UX, IBM AIX, SUN Solaris, Vmware, Citrix XEN Server.  10) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem).  11) Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności minimum 128 TB.  12) Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji  13) Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Off-loaded Data Transfer i Space Reclamation w środowiskach MS Windows  14) Wraz z macierzą należy zapewnić dostęp do bezpłatnych aktualizacji (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego macierzy w całym okresie obowiązywania gwarancji). | TAK / NIE |
| Konfiguracja, zarządzanie | 1. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 2. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. | TAK / NIE |
| Gwarancja | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty urządzenia. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. | TAK / NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Urządzenie NAS z oprogramowaniem do tworzenia kopii zapasowych (backup)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Obudowa do montażu w szafie rack 19” o wysokości maksymalnie 2U, w komplecie z szynami do montażu | TAK / NIE |
| Pamięć RAM | Zainstalowane co najmniej 4 GB pamięci RAM. Możliwość rozbudowy do 32 GB pamięci RAM lub więcej. | TAK / NIE |
| Obsługa dysków | Ilość kieszeni dysków: co najmniej 8 (możliwość rozbudowy do 12 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 12 dysków).  Obsługiwane typy dysków: 3,5” SATA HDD, 2,5” SATA HDD, 2,5” SATA SSD  Możliwość zainstalowania karty SSD M.2. | TAK / NIE |
| Zamontowane dyski | Zamontowane co najmniej 6 dysków o pojemności co najmniej 8 TB każdy, o prędkości obrotowej co najmniej 7200 rpm, prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin. | TAK / NIE |
| RAID | Obsługa RAID co najmniej: pojedynczy dysk, RAID 0, 1, 5, 6, 10, JBOD | TAK / NIE |
| Porty | Wbudowany interfejs 1Gbit/s z min. czterema portami RJ-45 oraz funkcją agregacji łączy.  Porty USB 3.0 – co najmniej 2 szt.  Port eSATA – co najmniej 1 szt. | TAK / NIE |
| Gwarancja | Gwarancja na urządzenie wraz z dyskami co najmniej 24 miesiące. |  |
| Oprogramowanie | Wymagane jest dostarczenie licencji na oprogramowanie do tworzenia kopii zapasowych (backup)bez ograniczeń czasowych. Licencje pozwalające na ochronę minimum:   * wirtualnych maszyn pracujących na oferowanej platformie wirtualizacji serwerów i pracujących pod kontrolą oferowanych systemów operacyjnych oraz systemów z rodziny Microsoft Windows Server i Linux, * serwerów fizycznych pracujących pod kontrolą oferowanych systemów operacyjnych oraz systemów z rodziny Microsoft Windows Server i Linux.   Dostarczone licencje muszą umożliwiać backup środowiska wirtualnego składającego się z co najmniej dwóch serwerów 2-procesorowych i co najmniej 30 maszyn wirtualnych.  Oprogramowanie musi współpracować z infrastrukturą VMware w wersjach 6.0, 6.5, 6.7, 7.0 oraz Microsoft Hyper-V 2012, 2012 R2, 2019 oraz 2022  Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.  Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.  Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.  Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.  Oprogramowanie musi tworzyć “samowystarczalne” archiwa, do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.  Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental).  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.  Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy aktualizowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.  Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania wykonania kopii migawkowej (snapshot).  Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).  Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.  Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania  Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).  Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej  Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.  Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w oferowanym środowisku wirtualizacyjnym i być dostępna dla oferowanej macierzy.  Oprogramowanie musi posiadać wsparcie dla oferowanego środowiska wirtualizacyjnego potwierdzone odpowiednią certyfikacją.  Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.  Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).  Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.  Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.  Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).  Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).  Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.  Dodatkowo dla środowiska vSphere i HyperV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)  Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami  Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre  Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików  Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.  Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:   * Dla systemów Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs * Dla systemów Windows: NTFS, FAT, FAT32, ReFS   Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.  Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.  Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.  Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.  Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN  Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.  Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.  Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.  Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla dwóch dostawców.  Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. | TAK / NIE  Producent, nazwa oprogramowania: ………………………………………………………………… |

## Przełączniki sieciowe

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Przełącznik wielowarstwowy L2/L3, zarządzany | TAK / NIE |
| Obudowa | Do montażu w szafie rack 19”, wysokość 1U | TAK / NIE |
| Porty | 48 portów 10/100/1000BaseT RJ-45, uplink 4 x 10G SFP+  Port konsoli USB Type-B/RJ45  Porty dostępowe przełącznika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet) | TAK / NIE |
| Funkcjonalność | Obsługa protokołu NTP  Funkcje DHCP server, DHCP relay  Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping  Blokowanie Head of Line (HOL)  Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)  Zapobieganie atakom DoS  Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6  Obsługa funkcji Plug & Play  Przycisk reset | TAK / NIE |
| Wydajność | Przepustowość przełącznika (switching bandwidth) 170 Gb/s  Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 130 Mpps  Pamięć DRAM – 512 MB | TAK / NIE |
| Obsługa standardów komunikacyjnych | IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet | TAK / NIE |
| Zarządzanie | Port konsoli  Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją  Obsługa protokołów SNMPv3, SSHv2, https, syslog  Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgrade’u oprogramowania urządzenia  Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki  Obsługa protokołu LLDP i LLDP-med. | TAK / NIE |
| Gwarancja | Co najmniej pięcioletnia gwarancja producenta. | TAK / NIE |

## Oprogramowanie do nadzoru nad siecią LAN

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane oprogramowanie – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Licencja | Wymagane dostarczenie licencji bezterminowej umożliwiającej nadzór nad siecią obejmującą 65 stanowisk roboczych | TAK / NIE |
| Wymagania ogólne | * + agent przeznaczony dla stacji roboczych pracujących pod kontrolą systemu Windows 8.1, 10, 11   + ochrona agenta przed usunięciem   + pakiet narzędzi diagnostycznych   + alarmy zdarzenie-akcja   + powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)   + zarządzanie hierarchią użytkowników (w tym import z AD)   + raporty dla użytkowników, urządzeń, oddziałów, map sieci   + jednoczesna praca wielu administratorów, dziennik dostępu administratorów   + zarządzanie uprawnieniami wielu administratorów   + zarządzanie grupami (tworzenie, przypisywanie użytkowników)   + menu kontekstowe z możliwością definiowania własnych narzędzi   + prezentowanie wybranych danych w przeglądarce internetowej za pomocą widgetów   + responsywne widgety, zarządzanie rozmiarem siatki widgetów   + automatyczne odświeżanie dashboardów   + udostępnianie dashboardów w trybie tylko do odczytu | TAK / NIE |
| Monitoring sieci | * + skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP   + interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne   + jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu   + serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)   + liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.   + działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń   + liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)   + kompilator plików MIB   + obsługa pułapek SNMP   + routery i switche: mapowanie portów   + obsługa komunikatów syslog   + alarmy zdarzenie - akcja   + powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (np.: uruchomienie programu, restart komputera)   + raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci) | TAK / NIE |
| Inwentaryzacja - zarządzanie zasobami IT | * + audyt inwentaryzacji sprzętu i oprogramowania   + wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach   + zdalny dostęp do managera plików z możliwością usuwania plików użytkownika   + informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej   + szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej   + zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI   + alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych   + lista kluczy oprogramowania Microsoft   + aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR   + możliwość archiwizacji i porównywania audytów   + monitorowanie harmonogramu zadań Windows   + Bezpieczeństwo danych i zarządzanie użytkownikami   + minimalizacja zjawiska cyberslackingu i zwiększenie wydajności pracowników   + redukcja kosztów wydruku   + blokowanie stron WWW   + blokowanie uruchamianych aplikacji   + monitorowanie wiadomości e-mail (nagłówki) - antyphishing   + szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)   + użytkowane aplikacje (aktywnie i nieaktywnie)   + odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)   + audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków   + użycie łącza: generowany przez użytkowników ruch sieciowy   + statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)   + zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)   + blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE   + zarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników) | TAK / NIE |
| Helpdesk - pomoc techniczna | * + system raportów   + powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym   + baza zgłoszeń z wyszukiwarką   + baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube   + interfejs webowy   + wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych   + komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu   + zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury   + dwukierunkowa wymiana plików   + zarządzanie procesami Windows z poziomu okna informacji o urządzeniu   + zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)   + procesowanie zgłoszeń z wiadomości e-mail   + integracja bazy użytkowników z Active Directory   + zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont) | TAK / NIE |
| Kontrola dostępu do danych | * + zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami   + informacje o urządzeniach podłączonych do danego komputera   + lista wszystkich urządzeń podłączonych do komputerów w sieci   + audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych   + zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników   + centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory   + integracja bazy użytkowników i grup z Active Directory   + alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym |  |
| Wykorzystanie czasu | * + lista aplikacji używanych przez pracowników z możliwością filtrowania, przypisywania do wybranych kategorii i nadawania im odpowiednich statusów   + podgląd aplikacji używanych w grupie bądź przez indywidualnego użytkownika w dowolnym czasie   + dodawanie wyjątków przez administratora grupy, wskazujących, że dana aplikacja w tej grupie jest uznawana za produktywną   + możliwość wskazywania przez administratora statusów konkretnych aplikacji: produktywna / neutralna / nieproduktywna   + grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne / nieproduktywne / neutralne   + widok najczęściej używanych aplikacji produktywnych, nieproduktywnych i neutralnych w dowolnie wybranym okresie czasu   + definiowanie minimalnego progu produktywności (czasu spędzonego w aplikacjach produktywnych) i maksymalnego progu nieproduktywności (czasu spędzonego w aplikacjach nieproduktywnych)   + cykliczne alerty wysyłane mailem o przekroczeniu zdefiniowanych progów produktywności   + możliwość ustalania okresu, po którym dane mają być usuwane z modułu   + lista kontaktów w organizacji z wbudowaną wyszukiwarką   + podgląd zrzutu ekranu wybranego użytkownika dostępny dla menedżerów i administratorów   + czas prywatny - możliwość wyłączenia analizy aktywności w czasie używania służbowego komputera do celów prywatnych. |  |

## Usługi wdrożeniowe

W ramach zamówienia Wykonawca zrealizuje usługi instalacji i konfiguracji zakupionego sprzętu i oprogramowania oraz przeniesienia oprogramowania i baz danych ze dotychczas eksploatowanych serwerów.

Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.

Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.

Zamawiający wymaga wykonania następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:

1. Sporządzenia planu wdrożenia, według którego nastąpi jego realizacja. Plan ten musi być uzgodniony z Zamawiającym i uwzględniać wszystkie aspekty wdrożenia. W szczególności:
   1. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych;
   2. schematy połączeń;
   3. mechanizmy działania głównych elementów sprzętowych;
      1. sieć LAN,
      2. klaster wirtualizacyjny,
      3. system backupu i archiwizacji danych,
      4. system serwerowy,
      5. system macierzowy;
   4. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności;
   5. sposób odbioru uzgodniony z Zamawiającym;
   6. listę i opisy procedur, stosowanie których gwarantuje Zamawiającemu prawidłowe działanie systemu;
   7. opis przypadków, w których projekt dopuszcza niedziałanie systemu.

Montaż i fizyczne uruchomienie systemu

Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:

1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniu wskazanym przez Zamawiającego.
2. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
4. Podłączenie wszystkich elementów do infrastruktury Zamawiającego.
5. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
6. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
7. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
8. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
9. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:
   1. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
   2. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.
   3. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
   4. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
10. Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji.
11. Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów)
12. Urządzenie NAS należy przyłączyć do infrastruktury Zamawiającego celem stworzenia miejsca na przechowywanie danych backupu.

Instalacja i konfiguracja oprogramowania

1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji.
2. Instalacja i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych.
3. Instalacja i konfiguracja systemów operacyjnych dla serwerów wirtualnych.
4. Instalacja i konfiguracja oprogramowania bazodanowego.

Konfiguracja sieci LAN

1. Konfiguracja dostarczanych przełączników w zakresie:
   1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
   2. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów.
   3. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).
   4. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.
      1. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink.
      2. Z wykorzystaniem połączeń światłowodowych oraz miedzianych.
      3. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu.
      4. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps.
   5. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.
   6. Konfiguracja routingu pomiędzy sieciami VLAN na posiadanym urządzeniu UTM.
   7. Zamawiający wymaga instalacji i konfiguracji Oprogramowania do nadzoru nad siecią LAN będącego przedmiotem zamówienia.
   8. Testowanie obsługi ruchu sieciowego.
   9. Testowanie skuteczności zabezpieczeń.

Rekonfiguracja elementów bezpieczeństwa sieciowego

1. Urządzenie firewall - rekonfiguracja posiadanego przez Zamawiającego urządzenia UTM (FortiGate 60E) w nw. zakresie.
   1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
   2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
   3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, kontrola aplikacji, filtrowanie WWW, filtrowanie e-mail).
   4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu.
   5. Konfiguracja dostarczonych systemów firewall:
      1. Konfiguracja podstawowych parametrów;
      2. Konfiguracja translacji adresów NAT;
      3. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze itp.;
      4. Konfiguracja inspekcji określonych protokołów sieciowych;
      5. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
      6. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
      7. Testowanie działania bramy.
   6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
      1. Konfiguracja podstawowych parametrów
      2. Konfiguracja mechanizmów ochrony określonych; sieci VLAN przez moduł wykrywania włamań;
      3. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
      4. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
      5. Testowanie działania ochrony IPS.
   7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
      1. Przypisanie adresu IP do zarządzania;
      2. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3;
      3. Definicja reguł filtrowania/blokowania;
      4. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny.
   8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.
   9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.
   10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.
   11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC
   12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
       1. kontrola dostępu - zapora ogniowa klasy Stateful Inspection;
       2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar;
       3. ochrona przed atakami - Intrusion Prevention System [IPS/IDS];
       4. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM;
       5. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP);
       6. kontrola pasma oraz ruchu [QoS, Traffic shaping];
       7. Kontrola aplikacji oraz rozpoznawanie ruchu P2P;
       8. Ochrona przed wyciekiem poufnej informacji (DLP);
       9. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL);
       10. Inspekcja ruchu SSL;
       11. Ochrony przez atakami na stacje klienckie;
       12. Kontrola pasma.
   13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi (np.: RCIM).
   14. Konfiguracja logowania i raportowania.

Serwer SMTP

1. Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.
2. Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z urządzeń sieciowych, serwerów, macierzy dyskowej, oprogramowania do tworzenia kopii zapasowych, oprogramowania do wirtualizacji oraz aplikacji.
3. Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.

Uruchomienie środowiska wirtualizacyjnego

1. Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:
2. Aktywacja licencji dostarczonego oprogramowania do wirtualizacji na stronie producenta.
3. Przygotowanie serwerów do instalacji oprogramowania do wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
4. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
5. Instalacja oprogramowania do wirtualizacji na dostarczonych serwerach.
6. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania do wirtualizacji oraz przez producenta serwerów.
7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) (n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
8. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Zamawiającego. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) (n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
9. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
10. Przygotowanie koncepcji wirtualizacji fizycznych maszyn.
11. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
12. Konfiguracja klastra wysokiej dostępności:
    1. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
    2. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
    3. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
13. Weryfikacja działania klastra wysokiej dostępności.
14. Migracja istniejącej infrastruktury do środowiska wirtualnego.
15. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową
16. Konfiguracja powiadomień o krytycznych zdarzeniach (email).

System kopii zapasowych (backupu)

1. Instalacja oprogramowania do tworzenia kopii zapasowych dostarczonego w pakiecie z urządzeniem NAS.
2. Aktywacja oraz instalacja niezbędnych licencji.
3. Konfiguracja stacji zarządzającej.
4. Dołączenie klientów do systemu backupu.
5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:
   1. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
   2. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
   3. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
   4. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
   5. musi istnieć możliwość odtworzenia:
      1. całej wirtualnej maszyny;
      2. dysku wirtualnej maszyny;
      3. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa).
6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej:
   1. Nazwę zadania backupu;
   2. Status zakończenia zadania backupu (powodzenie/niepowodzenie);
   3. Długość trwania zadania backupu;
   4. Ilość zapisanych danych.
7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach:
   1. Błąd urządzenia;
   2. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi;
   3. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi;
   4. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi;
   5. Zdarzenia dotyczące licencji;
   6. Zapełnienia mail-slotu.
8. Uruchomienie testowych zadań backupu
9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email
10. Uruchomienie testowych zadań odtworzenia danych
11. Miejscem przechowywania kopii zapasowych ma być dostarczane urządzenie NAS.
12. Na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym.
13. System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na urządzeniu NAS.

Usługa katalogowa

1. Wymagane zaplanowanie liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików zapewniającej, w przypadku awarii pojedynczego serwera, ciągły dostęp do usługi katalogowej, a w szczególności do mechanizmów uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym.
2. Instalacja systemu operacyjnego serwerów. Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
3. Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.
4. Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.
5. Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:
   1. Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości;
   2. Śledzenie zmian dotyczących tworzenia, usuwania obiektów.
6. Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
7. Konfiguracja globalnej polityki haseł dla domeny:
   1. Hasło musi zawierać minimum 8 znaków;
   2. Maksymalny czas ważności hasła: do ustalenia z Zamawiającym;
   3. Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym;
   4. Hasło musi spełniać zasady złożoności.
8. Konfiguracja polityki haseł dla kadry zarządzającej:
   1. Hasło musi zawierać minimum 10 znaków;
   2. Maksymalny czas ważności hasła: 30 dni;
   3. Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni;
   4. Hasło musi spełniać zasady złożoności.
9. Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.
10. Szczegółowe dane zostaną przekazane na etapie konfiguracji.
11. Stworzenie skryptów służących do tworzenia struktury usługi katalogowej. Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje opracowanie przez Wykonawcę skryptów ułatwiających te zadania.
12. Opracowane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące ich działanie. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi.
13. Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.
14. Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows.
15. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby:
    1. Z wykorzystaniem skryptów logowania.
    2. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows 10 i nowszych. Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie.

Uruchomienie i skonfigurowanie serwera plików oraz wydruków

1. Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:
   1. Replikację multi-master z rozwiązywaniem konfliktów;
   2. Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.
2. Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.
3. Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów.
4. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.
5. Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego.
6. Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych.
7. Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji.
8. Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:
   1. Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder;
   2. Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder;
   3. Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.
9. Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.

Serwery uwierzytelniające

1. Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych.
2. Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.
3. Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę.
4. Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.
5. Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.

Dołączenie stacji roboczych do domeny

1. Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny (60 stacji roboczych). W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji).
2. Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows według założeń:
   1. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet;
   2. Administrator zatwierdza aktualizacje do instalacji;
   3. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu.
3. Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:
   1. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje;
   2. Kategorii aktualizacji;
   3. Grup komputerów;
   4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów;
   5. Zasad automatycznego zatwierdzania nowych aktualizacji;
   6. Mechanizmów raportowania (e-mail).

Przygotowanie infrastruktury PKI

1. Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 8.x, Windows 10 i Windows 11.
2. Wymagana przez Zamawiającego konfiguracja musi uwzględniać:
   1. Zaplanowanie i uruchomienie wewnętrznej struktury CA;
   2. Konfigurację szablonów certyfikatów;
   3. Wydanie certyfikatów dla serwerów oraz stacji roboczych;
   4. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów;
   5. Wskazanie wszystkich możliwych dróg publikacji list CRL;
   6. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji.

Testowanie i modyfikacja parametrów infrastruktury sieciowej

1. Testowanie mechanizmów bezpieczeństwa klastra serwera, środowiska wirtualizacyjnego.
2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN.
3. Testowanie dostępu publicznego do zasobów.
4. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu.
5. Testowanie autoryzowanego dostępu do wewnętrznych zasobów.
6. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach.

Migracja systemów informatycznych

1. Wykonawca przeniesie obecnie eksploatowane systemy informatyczne na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Systemy wraz z ich bazami danych muszą zostać przeniesione na nowe zasoby serwerowo-macierzowe.
2. W ramach migracji zostaną przeniesione nw. systemy:

Oprogramowanie Biura Usług Komputerowych Softres, Rzeszów

* 1. Moduł obsługi podatkowej wraz z księgowością podatkową
  2. Moduł ewidencji zwrotu podatku akcyzowego
  3. Moduł obsługi podatku od środków transportowych
  4. Moduł obsługi opłat za gospodarowanie opłatami komunalnymi
  5. Moduł finansowo-księgowy
  6. Moduł kasowy
  7. Moduł kadry
  8. Moduł ewidencja środków trwałych
  9. Moduł system ewidencja i rozliczanie opłat
  10. Broker komunikacyjny SUSerwis (integrator systemów dziedzinowych z EZD oraz portalami eusług: eVat, eNależności, eSPrawozdawczość)
  11. oraz: SIO Bestia
  12. Płatnik

1. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej co najmniej w pełnym zakresie danych i rejestrów systemów dziedzinowych.

Opracowane dokumentacji powykonawczej

1. Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie obszary będące przedmiotem usługi. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. W szczególności dokumentacja musi zawierać:
   1. Wszelkie zmiany w stosunku do planu wdrożenia z podaniem ich powodów.
   2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).
   3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
   4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.
   5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.