**Załącznik nr 8**

**Szczegółowy opis przedmiotu zamówienia**

Listopad 2022

Spis treści

[1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego. 3](#_Toc119673134)

[2 Wymagania gwarancyjne. 3](#_Toc119673135)

[3 Miejsce instalacji sprzętu i oprogramowania/systemu. 3](#_Toc119673136)

[4 Zestawienie zakresu dostaw i usług. 3](#_Toc119673137)

[4.1 Zestaw komputerowy wraz z oprogramowaniem – szt. 27 – wymagania minimalne 5](#_Toc119673138)

[4.2 Laptopy – szt. 4 – wymagania minimalne 10](#_Toc119673139)

[4.3 Oprogramowanie do backupu – szt.1 – wymagania minimalne 16](#_Toc119673140)

[4.4 Serwerowy system operacyjny – szt. 2 – wymagania minimalne 20](#_Toc119673141)

[4.5 Oprogramowanie bazodanowe – szt.2 – wymagania minimalne 22](#_Toc119673142)

[4.6 Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania. 26](#_Toc119673143)

[4.7 Diagnoza cyberbezpieczeństwa 36](#_Toc119673144)

# Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

1. Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
2. Całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

# Wymagania gwarancyjne.

**Sprzęt**

1. O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. dwuletnia gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
2. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych co najmniej jednym z wymienionych kanałów: telefon (w godzinach pracy Zamawiającego), e-mail serwis internetowy (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
3. Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego;

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

# Miejsce instalacji sprzętu i oprogramowania/systemu.

1. Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika na 1, w budynkach urzędu w miejscach wskazanych przez Zamawiającego.

# Zestawienie zakresu dostaw i usług.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Opis pozycji** | **Liczba jednostek** | **Długość gwarancji (minimum) [m-ce]** | **Uwagi** |
| 1. | Zestaw komputerowy wraz z oprogramowaniem | 27 szt. | 24  (kryterium oceny) | Zastąpienie obecnie używanych, wyeksploatowanych komputerów, pracujących pod kontrolą systemu operacyjnego, którego wsparcie zakończy się z początkiem 2023 r. przyczyni się do wzrostu bezpieczeństwa przetwarzanych danych oraz pozwoli na uniknięcie przestojów spowodowanych awarią sprzętu.  Parametry techniczne stacji (minimalne): RAM 8 GB, 256SSD, procesor, zintegrowana karta graficzna,  Monitor: min, 24’’, FHD  Klawiatura i mysz w zestawie, system operacyjny |
| 2. | Laptopy wraz z oprogramowaniem | 4 szt. | 24  (kryterium oceny) | Pozycja uwzględnia koszt zakupu laptopów dla pracowników urzędu. Urządzenia pozwolą na pracę zdalną w przypadku zaistnienia takiej potrzeby. Ponadto zastąpią one obecnie wykorzystywane laptopy, pracujące pod kontrolą systemu operacyjnego, którego wsparcie zakończy się z początkiem 2023 r., co wpłynie na zwiększenie bezpieczeństwa przetwarzanych danych oraz pozwoli na uniknięcie przestojów spowodowanych awarią sprzętu. Parametry planowane: komputer do zastosowań biurowych, min. 15’’ matryca, min. 8 GB RAM, min. 256 GB SSD, system operacyjny. |
| 3. | Oprogramowanie do backupu 10 maszyn | licencja dla 10 maszyn | 12 | Oprogramowanie umożliwi większą kontrolę nad procesem archiwizacji i przywracania danych oraz optymalne zarządzanie kopiami zapasowymi i miejscem przeznaczonym do ich przechowywania. Pozwoli m.in. walidację poprawności wykonania kopii zapasowej, czego nie umożliwi obecnie wykorzystywane oprogramowanie.  Zaplanowano zakup licencji wieczystej rozwiązania w celu umożliwienia wykonywania kopii zapasowych 10 maszyn. |
| 4. | Serwerowy system operacyjny | 2 szt. | Nd. | Pozycja dotyczy zakupu licencji na system operacyjny Windows Server 2019, co pozwoli na przeniesienie kontrolera domeny AD na system, posiadający wsparcie producenta w zakresie aktualizacji, w tym aktualizacji bezpieczeństwa. Konieczność zakupu konkretnej wersji systemu operacyjnego podyktowana jest faktem, że Starostwo dysponuje licencjami dostępowymi CAL dla tej właśnie wersji systemu w liczbie zapewniającej dostęp do zasobów serwera wszystkim pracownikom Starostwa, co pozwoli na racjonalne dysponowanie środkami finansowymi i pozwoli obniżyć koszty wdrożenia. Ponadto w/w system operacyjny wykorzystany zostanie do uruchomienia serwera do obsługi baz danych.  Przeniesienie danych na wspierany system operacyjny oraz wirtualizacja środowiska przyczynią się do zwiększenia bezpieczeństwa. |
| 5. | Oprogramowanie bazodanowe | 2 szt. | Nd. | Oprogramowanie bazodanowe używane obecnie przez Startostwo nie jest już wspierane przez producenta i nie otrzymuje aktualizacji.  Z uwagi na wykorzystywane w Starostwie oprogramowanie IT, które korzysta z baz danych MS SQL nie jest możliwa zmiana systemu służącego do obsługi bazy danych.  Z kolei ze względów bezpieczeństwa przetwarzanych danych, wskazane jest korzystanie z aktualnego oprogramowania, posiadającego wsparcie producenta, zwłaszcza w zakresie aktualizacji wykrytych luk i podatności.  Przeniesienie serwera bazy danych do nowoczesnego, zwirtualizowanego środowiska będzie miało korzystny wpływ zarówno w zakresie poprawy bezpieczeństwa, jak też wzrostu wydajności i optymalnego wykorzystania zasobów.  Zakup dwóch sztuk licencji wynika bezpośrednio z zapisów licencyjnych oprogramowania, zgodnie z którymi w przypadku instalacji na maszynie wirtualnej, konieczny jest zakup licencji na minimum cztery rdzenie, podczas gdy pojedyncza licencja, jest licencją na dwa rdzenie. |
| 6. | Instalacja i konfiguracja | 1 | 12 | Usługi obejmować będą:   1. Instalację i konfiguracje zakupionych urządzeń i oprogramowania. 2. Migrację danych ze starych maszyn do nowego środowiska zawirtualizowanego (migracja domeny AD oraz serwera baz danych). 3. Instruktaż dla administratorów 4. Wsparcie techniczne, nadzór autorski 12 miesięcy.   Łącznie przewidziano 50 godz. roboczych. |
| 7. | Diagnoza cyberbezpieczeństwa | 1 | Nd. | Nd. |

## Zestaw komputerowy wraz z oprogramowaniem – szt. 27 – wymagania minimalne

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Podzespół** | **Minimalne parametry** |
|  | Typ komputera | **Komputer stacjonarny** |
|  | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do zasobów lokalnej sieci komputerowej oraz usług sieci Internet, aplikacji graficznych wektorowych oraz rastrowych, a także danych multimedialnych. |
|  | Procesor | klasy x86, ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych, zapewniający wydajność procesora min. 17500 pkt. w teście Passmark CPU Mark (wyniki testu nie starsze niż z dnia 20.11.2022 r. i znajdujący się na liście <https://www.cpubenchmark.net/cpu_list.php>  Zamawiający dopuszcza wydruk w języku angielskim na podstawie art. 20 ust. 3 ustawy Pzp. |
|  | Płyta główna | * chipset dostosowany do oferowanego procesora * minimum 4 sloty pamięci * minimum 1 x PCI Express 3.0 x 4 * minimum 3 złącza SATA 6.0 Gb/s * minimum 1x M.2 dla dysku SSD o przepustowości 32Gbit/s * 1x USB (gniazdo bezpośrednio na płycie głównej) |
|  | Pamięć operacyjna RAM | * minimum 8 GB * minimalny rozmiar możliwego rozszerzenia obsługiwanej pamięci, zapewniony i potwierdzony przez producenta komputera:  128 GB |
|  | Porty w tylnej części komputera | Komputer musi posiadać:   * minimum 2 x Display Port 1.4 z obsługą funkcji Multi-Stream, * minimum 4 x USB, w tym co najmniej 2x USB 3.2 Gen 1 * minimum 1 port sieciowy RJ-45, * osobne porty audio line-in i line-out   Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB oraz VIDEO nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
|  | Porty w przedniej części komputera | Komputer musi posiadać:   * minimum 4 x USB, w tym min. 2x USB 3.2 Gen 1 * port audio do podłączenia słuchawek lub słuchawek z mikrofonem |
|  | Dysk twardy | * Minimum 256GB SSD z interfejsem M.2 NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego  zainstalowanego  na komputerze przez producenta, po awarii, do stanu fabrycznego (tryb OOBE dla systemu MS Windows) * Możliwość zamontowania w obudowie jednego dysku 3,5 cala. |
|  | Napęd optyczny | Nagrywarka DVD +/-RW |
|  | Karta dźwiękowa | Karta dźwiękowa zintegrowana z płytą główną, zgodna ze standardem High Definition 5.1 |
|  | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.5, OpenCL 2.1. |
|  | Karta sieciowa | Karta sieciowa 10/100/1000 Ethernet RJ-45, zintegrowana z płytą główną wspierająca obsługę technologii WoL oraz PXE. Zintegrowana karta sieciowa musi być wyposażona w diodę statusu informującą a aktywności połączenia oraz diodę informującą o prędkości połączenia. |
|  | BIOS | BIOS UEFI w wersji 2.6 lub wyższej. Możliwość odczytania z BIOS informacji o:   * modelu komputera, * numerze seryjnym, * AssetTag/IDTag * MAC Adres karty sieciowej, * wersja Biosu wraz z datą jego produkcji, * zainstalowanym procesorze, jego taktowaniu * ilości pamięci RAM wraz z taktowaniem i obłożeniem slotów   Możliwość z poziomu BIOS:   * wyłączenia selektywnego portów USB, minimum wyłączanie portów z przodu oraz wyłączanie portów z tyłu jako grup * wyłączenia selektywnego (pojedynczego) portów SATA, * zmiany pracy wentylatorów między trybem optymalizacji głośności lub temperatury, * ustawienia hasła: administratora, Power-On, HDD, * możliwość zbierania i przeglądania logów zdarzeń z informacją odnośnie godziny, daty i kodu błędu zdarzenia * ustawienie automatycznej aktualizacji BIOS z serwera producenta komputera |
|  | Klawiatura | Klawiatura USB w układzie polskim programisty (105 klawiszy) z kablem o długości min. 1,8 m lub klawiatura bezprzewodowa. |
|  | Mysz | Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m lub mysz bezprzewodowa. |
|  | Obudowa | * Typu desktop (SFF) przystosowana do pracy w pionie i w poziomie, z obsługą kart PCI Express wyłącznie o niskim profilu;. * Suma wymiarów obudowy, nie może przekroczyć: 700 mm, najkrótszy z wymiarów nie większy niż: 90 mm * Możliwość zainstalowania dedykowanego przez producenta filtra przeciwkurzowego; * Głośność jednostki centralnej nie może przekraczać 22 dB, mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego rotującego. |
|  | Zasilanie | Zasilacz o mocy nie mniejszej niż 280 W, o sprawności 94% przy obciążeniu 50%. |
|  | Bezpieczeństwo i funkcje zarządzania | 1. Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera. 2. TPM 2.0. 3. Możliwość wbudowania czytnika SmartCard 4. System diagnostyczny działający bez udziału systemu operacyjnego, czy też jakichkolwiek dołączonych urządzeń na zewnątrz czy też wewnątrz komputera, umożliwiający otrzymanie informacji o:  * modelu, oznaczeniu  i numerze seryjnym komputera, * pojemności zainstalowanej pamięci RAM   Oprogramowanie diagnostyczne musi umożliwiać:   * wykonanie testu pamięci RAM, * wykonanie podstawowego testu prawidłowej pracy CPU * wykonanie testu dysku twardego.   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera (Zaimplementowany w sprzętowym mikrokodzie płyty głównej) |
|  | Sterowniki  i oprogramowanie | Zapewnienie na dedykowanej stronie internetowej producenta dostępu do najnowszych sterowników i uaktualnień, realizowane poprzez podanie numeru seryjnego/modelu urządzenia  Oprogramowanie producenta komputera posiadające funkcje zarządzania sterownikami (wykrywanie i instalowanie aktualizacji). |
|  | Certyfikaty  i oświadczenia | 1. Producent komputera musi posiadać ISO 9001 co najmniej w zakresie projektowania, produkcji i serwisu komputerów. 2. Producent komputera musi posiadać ISO 14001, co najmniej w zakresie projektowania i produkcji. 3. Oferowane komputery stacjonarne muszą posiadać europejską deklarację zgodności CE. 4. Certyfikat poprawnej współpracy z zaoferowanym systemem operacyjnym - do oferty dołączyć wydruk ze strony producenta oprogramowania systemowego. |
|  | Zainstalowane oprogramowanie systemowe | Zainstalowany 64-bitowy system operacyjny w polskiej wersji językowej .  Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  *Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.*  System operacyjny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 6. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 7. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 10. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4  i v6. 11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 13. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 14. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 15. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 16. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 18. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 19. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 21. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 22. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 23. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 24. Mechanizmy logowania do domeny w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 25. Mechanizmy wieloelementowego uwierzytelniania. 26. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 27. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 28. Wsparcie dla algorytmów Suite B (RFC 4869). 29. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 30. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 31. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 32. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 33. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 34. 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. 35. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 36. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 37. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 38. Udostępnianie modemu. 39. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 40. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 41. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa  (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 42. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 43. Wbudowany mechanizm wirtualizacji typu hypervisor, 44. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 45. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera,  z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 46. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 47. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 48. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
|  | Gwarancja – zgodnie z wymaganiami i kryteriami | Min. 24 miesiące świadczonej  w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym  - wówczas koszt transportu do i z naprawy pokrywa Wykonawca.  Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela |
| Monitor | | |
|  | Ekran | 23,8 cala o rozdzielczości natywnej minimum 1920x1080 pikseli, maksymalny rozmiar piksela 0.275 mm, matryca matowa, pokryta powłoką 3H, technologia matrycy IPS |
|  | Parametry obrazu | Odwzorowanie 16.7 miliona kolorów, kontrast typowy 1000:1,  jasność min. 250 cd/m2, czas reakcji matrycy max. 5ms, kąty widzenia pionowe/poziome minimum 178/178 stopni |
|  | Wejścia wideo i inne | 1x DP, 1x DVI-D, 1x D-SUB, wejście/wyjście audio |
|  | Obudowa i  regulacja monitora | Pochylenie ekranu w zakresie -5° / +22°(tzw. Tilt), zintegrowany zasilacz i głośniki stereo o mocy minimum 2W każdy, możliwość regulacji głośności z menu OSD monitora, złącze Kensington Lock, złącze montażu na ścianie w standardzie VESA, regulacja wysokości, dominujący kolor obudowy: czarny |
|  | Funkcje zarządzana energią i parametrami wyświetlania obrazu | Technologia zapewniająca  zużycie energii przez monitor w trybie power save na poziomie 0.2W pozwalająca na redukcję ogólnego zużycia energii przez monitor (bez konieczności manualnego wyłączania monitora przez użytkownika), zgodność z normą Energy Star 8.0, zużycie energii przy ustawieniach EPA max. 14W |
|  | Menu monitora | Regulacja głośności  Regulacja jasności  Regulacja kontrastu  Regulacja koloru (sRGB, 5000K, 6500K, 7500K, Użytkownika (R,G,B)  Menu w języku polskim oraz angielskim. |
|  | Kable | kabel sygnałowy cyfrowy o długości minimum 1.8m, kabel zasilający o długości minimum 1,8m, kabel audio |

## Laptopy – szt. 4 – wymagania minimalne

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Wymagane parametry techniczne** |
|  | Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
|  | Matryca | Matryca o przekątnej 15.6” z powłoką przeciwodblaskową i rozdzielczością 1920 x 1080. Jasność matrycy 250 cd/m2, kontrast min. 700:1. |
|  | Wydajność | Wynik testu procesora potwierdzający, że oferowany procesor osiągnął w teście PassMark Performance Test, co najmniej 10 000 punktów w kategorii Average CPU Mark (wyniki testu nie starsze niż z dnia 20.11.2022 r.) Wynik dostępny na stronie: <https://www.cpubenchmark.net/cpu_list.php>  Zamawiający dopuszcza wydruk w języku angielskim na podstawie art. 20 ust. 3 ustawy Pzp. |
|  | Pamięć RAM | 16GB możliwość rozbudowy do min 32GB, min. jeden wolny slot pamięci na dalszą rozbudowę |
|  | Pamięć masowa | 256GB SSD NVMe |
|  | Karta graficzna | Zintegrowana z procesorem |
|  | Klawiatura | Klawiatura w układzie US - QWERTY z wydzieloną klawiaturą numeryczną oraz z wbudowanym w klawiaturze podświetleniem. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. |
|  | Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2 x 2W.  Czytnik kart multimedialnych w formacie microSD,  Złącze audio typu combo (słuchawki i mikrofon) |
|  | Łączność bezprzewodowa | Karta Wireless AX + Bluetooth 5.1 |
|  | Bateria i zasilanie | Bateria min. 3-cell [min. 41Wh]. Umożliwiająca jej naładowanie w czasie max. 4 godzin. |
|  | Waga | Waga max 2kg z baterią.  Suma wymiarów notebooka nie większa niż 622mm (mierzone po krawędziach) |
|  | Obudowa | Kolor przeważający szary lub czarny |
|  | BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego (wmontowanego na stałe). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i maksymalnej osiąganej prędkości, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag, nie podlegające skasowaniu nawet po aktualizacji BIOS.  Funkcja logowania się do BIOS na podstawie hasła użytkownika i administratora (hasła niezależne), możliwość ustawienia haseł administratora oraz użytkownika składających się z małych liter, dużych liter, cyfr, znaków specjalnych.  BIOS zawierający informację o stanie naładowania baterii, mocy podpiętego zasilacza, ponadto możliwość zarządzania trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
|  | Certyfikaty | Certyfikat ISO9001 lub równoważny dla producenta sprzętu.  Certyfikat ISO 14001 lub równoważny dla producenta sprzętu.  Deklaracja zgodności CE.  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki  Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym.  Certyfikat EnergyStar lub równoważny. |
|  | Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych i dodatkowych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. |
|  | Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje 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. |
|  | System operacyjny | Zainstalowany 64-bitowy system operacyjny w polskiej wersji językowej .  Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.  *Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.*  System operacyjny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 6. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 7. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 10. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4  i v6. 11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 13. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 14. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 15. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 16. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 18. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 19. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 21. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 22. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 23. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 24. Mechanizmy logowania do domeny w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 25. Mechanizmy wieloelementowego uwierzytelniania. 26. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 27. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 28. Wsparcie dla algorytmów Suite B (RFC 4869). 29. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 30. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 31. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 32. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 33. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 34. 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. 35. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 36. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 37. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 38. Udostępnianie modemu. 39. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 40. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 41. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa  (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 42. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 43. Wbudowany mechanizm wirtualizacji typu hypervisor, 44. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 45. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 46. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 47. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.  * Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
|  | Oprogramowanie dodatkowe | Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające :   * określenie preferencji aktualizacji * ustawienie priorytetu aktualizacji * użycia opcji planowania aktualizacji bieżących wersji sterowników,   Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :                   a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja                  f.  wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.   * wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne * możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. * rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr ) * sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania ) * dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml * raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
|  | Porty i złącza | Wbudowane porty i złącza: 1 x HDMI 1.4, 1x RJ-45, 1 x USB 2.0, 2 x USB 3.2 typu A, w tym jeden dosilony, 1x USB 3.2 gen 2 typu C, port zasilania, 1 x RJ-45, gniazdo linki zabezpieczającej. |
|  | Wsparcie techniczne | 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) |
|  | Warunki gwarancyjne | Gwarancja producenta świadczona na miejscu u klienta min. 24 miesiące.  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera.  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) |

## Oprogramowanie do backupu – szt.1 – wymagania minimalne

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Wymagania ogólne** | | Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 10 VM.  Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7, 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 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 Manger, 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. | | **Całkowite koszty posiadania** | | 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 musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. | | Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania 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 snapshota. | | 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. | | **Wymagania RPO** | | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej | | Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. | | 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 posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. | | 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. | | Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability) | | 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) | | **Wymagania RTO** | | 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 Hyper-V 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 umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. | | 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: | | o    Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs | | o    BSD: UFS, UFS2 | | o    Solaris: ZFS, UFS | | o    Mac: HFS, HFS+ | | o    Windows: NTFS, FAT, FAT32, ReFS | | o    Novell OES: NSS | | 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 dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. | | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), | | Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska | | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych | | Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska | | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych | | Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. | | 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 oraz migrację online 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 | | **Ograniczenie ryzyka** | | 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 Windows Defender, Symantec Protection Engine oraz ESET NOD32. | | Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. | | **Monitoring** | | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich | | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie | | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. | | System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware | | System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter | | System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn | | System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel | | System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk | | System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora | | System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów | | System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) | | System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna | | System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego | | System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta | | System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. | | System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. | | System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware | | System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x | | **Raportowanie** | | System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 | | System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. | | System musi być certyfikowany przez VMware i posiadać status „VMware Ready” | | System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V | | System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF | | System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc | | System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach | | System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów | | System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych | | System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych | | System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury | | System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta | | System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. | | System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. | | System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware | | System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) | | System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie | |

## Serwerowy system operacyjny – szt. 2 – wymagania minimalne

|  |
| --- |
| UWAGA:  Zamawiający dysponuje obecnie licencjami CAL do systemu Windows Serwer 2019. W związku z powyższym wymaga dostawy rozwiązania pozwalającego na wykorzystanie posiadanych licencji. W przypadku dostawy rozwiązania innego (równoważnego) wraz z dostawą systemu operacyjnego wymaga również dostawy licencji CAL (dla użytkownika)w ilości 100 szt.  Wymogi wobec systemu:  Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku złożonym z klastra dwóch serwerów dysponujących łącznie 32 rdzeniami CPU. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   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:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i nowszych.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. 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:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   1. 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. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

## Oprogramowanie bazodanowe – szt.2 – wymagania minimalne

|  |
| --- |
| Uwaga:  Starostwo Powiatowe używa obecnie oprogramowania dziedzinowego m.in. firm: Nefeni (Proton, Besti@), Softres (Sprawny Urząd), Utal,, które zgodnie z instrukcją producenta wymaga bazy danych MS SQL. Zamawiający wymaga zatem dostawy systemu bazodanowego umożliwiającego prawidłową pracę posiadanego oprogramowania. Zamawiający nie zawęża rodzajów dostarczanego oprogramowania. Jednak w przypadku zaoferowania bazy innej niż wskazana przez producenta systemu dziedzinowego Wykonawca jest zobowiązany dokonać integracji zaoferowanej bazy z systemami oraz uzyskać potwierdzenie producentów oprogramowania że zaoferowane rozwiązanie umożliwi prawidłową pracę oprogramowania.  W każdym wypadku Zamawiający wymaga dostawy oprogramowania bazodanowego o poniższych parametrach:  System bazodanowy (SBD) typ I licencjonowany na rdzenie procesora (licencja na 4 rdzenie) musi spełniać następujące wymagania poprzez wbudowane mechanizmy:   1. Możliwość wykorzystania SBD 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 – SBD 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 - SBD 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 - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania). 6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. 7. Wysoka dostępność - SBD 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 SBD), * 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 - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD 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 - SBD 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 - SBD 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 - SBD 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 - SBD 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 - SBD 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 - SBD 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 SBD, * 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 - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. 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 - SBD 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 SBD 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 - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych. 5. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD 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 SBD, wprowadzeniu zmian sprzętowych serwera. 6. System transformacji danych - SBD 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 - SBD 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) - SBD 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 - SBD 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. SBD 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. SBD 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). |

## Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.

|  |  |  |
| --- | --- | --- |
| **Instalacja i konfiguracja.** | | |
|  | Usługi | Celem prac jest modernizacja środowiska teleinformatycznego, na potrzeby realizacji usług publicznych, zbudowanego w oparciu o istniejące i dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.  Część sprzętowa powinna zostać oparta na modernizowanym systemie wirtualizacji zasobów IT.  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.  W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową.  Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:   * 1. Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.   2. Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać 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: * sieć LAN * klaster wirtualizacyjny * system backupu i archiwizacji danych * system serwerowy   + 1. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności     2. sposób odbioru uzgodniony z Zamawiającym     3. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu     4. opis przypadków, w których projekt dopuszcza niedziałanie systemu     5. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą   Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia. |
|  | 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. Urządzenia powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 2. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 3. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 5. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji |
|  | Instalacja i konfiguracja oprogramowania | 1. Instalacja i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych. 2. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). Na potrzeby systemu domenowego oraz dla innych serwerów wirtualnych. |
|  | Migracja danych | Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych (w szczególności Proton i Sprawny Urząd wraz z bazami danych i zachowaniem istniejącej integracji z innymi systemami) na nowe rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów.  Dane (maszyny, systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowe.  Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych. |
|  | System backupu | 1. Instalacja oprogramowania zarządzającego wykonywaniem kopii zapasowych. 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system 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 jest:     1. serwer backupu.     2. 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   System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu. |
|  | Usługa katalogowa. | Instalacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania. |
|  | Zaplanowanie liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików | Taka liczba serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym. |
|  | Wersja systemu operacyjnego serwerów | Zastosowany system operacyjny musi zapewniać, co najmniej:   1. możliwość uruchomienia usługi katalogowej w trybie usługi 2. możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń 3. możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń) 4. możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI 5. możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych |
|  | 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. |
|  | Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej | 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.  Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.  Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do:   1. Resetowania haseł użytkowników 2. Odblokowywania kont użytkowników 3. Zmiany atrybutów „Display Name” oraz „Last name”   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   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). |
|  | Konfiguracja polityki haseł oraz polityki blokowania kont | 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   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   Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.  Szczegółowe dane zostaną przekazane na etapie konfiguracji. |
|  | 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 stworzenia przez Wykonawcę skryptów ułatwiających te zadania.  Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:   1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej:    1. ścieżki i nazwy pliku wejściowego    2. ścieżki i nazwy pliku logującego    3. ścieżki i nazwy pliku wyjściowego (właściwego skryptu)    4. nazwy FQDN domeny    5. nazwy NetBIOS domeny    6. nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty    7. ścieżek do udziałów dyskowych SHARE1 oraz SHARE2 2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych 3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu 4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G\_Nazwa\_Jednoski\_Organizacyjnej 5. Skrypt tworzy foldery:    1. \\DOMENA\Public\SHARE1    2. \\DOMENA\Public\SHARE2   Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2.   1. Skrypt tworzy podkatalogi: [\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE1/Nazwa_Jednostki_Organizacyjnej) oraz [\\DOMENA\Public\SHARE2\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE2/Nazwa_Jednostki_Organizacyjnej) 2. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń:    1. [\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE1/Nazwa_Jednostki_Organizacyjnej):       1. Administratorzy Domeny – Pełna kontrola       2. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej       3. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu       4. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze    2. [\\DOMENA\Public\Share2\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/Share2/Nazwa_Jednostki_Organizacyjnej):       1. Administratorzy Domeny – Pełna kontrola       2. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej       3. Użytkownicy Uwierzytelnieni - Odczyt       4. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu       5. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 3. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 4. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania   Założenia skryptu tworzącego nowe konta użytkowników:   1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej:    1. ścieżki i nazwy pliku wejściowego    2. ścieżki i nazwy pliku logującego    3. ścieżki i nazwy pliku wyjściowego (właściwego skryptu)    4. nazwy FQDN domeny    5. nazwy NetBIOS domeny    6. nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty    7. ścieżki do udziału sieciowego HOME    8. litery dysku katalogu domowego 2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie:   NazwaUzytkownika;Imie;Nazwisko:Haslo;Dzial;NumerTelefonu   1. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego 2. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania 3. Skrypt tworzy katalog [\\DOMENA\HOME\NazwaUzytkownika](file://DOMENA/HOME/NazwaUzytkownika) 4. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń:    1. Administratorzy Domeny – Pełna kontrola    2. Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika    3. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu    4. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 5. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową 6. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 7. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania 8. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom.   Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi.  Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów. |
|  | Skonfigurowanie mapowania zasobów sieciowych | Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows.  Mapowane mają być między innymi zasoby:  \\DOMENA\Public\SHARE1  \\DOMENA\Public\SHARE2  Oraz określone przez Zamawiającego drukarki sieciowe.  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 Vista 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 | Zamawiający wymaga uruchomienie oraz skonfigurowanie serwerów plików oraz serwerów wydruków tak, aby były spełnione poniższe założenia:  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:   * Replikację multi-master z rozwiązywaniem konfliktów * Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.   Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.  Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów.  Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.  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.  Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych.  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.  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.   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 | Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD..  Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.  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.  Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.  Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie. |
|  | Dołączenie stacji roboczych do domeny | Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny. 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). |
|  | Uruchomienie usług umożliwiającą instalację i zarządzanie aktualizacjami stacji roboczych Windows | 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   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 (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST) 4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów 5. Zasad automatycznego zatwierdzania nowych aktualizacji. 6. Mechanizmów raportowania (email) |
|  | Przygotowanie infrastruktury PKI | Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10, Windows 11.  Wymagana przez Zamawiającego konfiguracja zawiera co najmniej:   1. Zaplanowanie i uruchomienie wewnętrznej struktury CA 2. Konfiguracja 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. |
|  | Asysty stanowiskowe | Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.  Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.  Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego. |
|  | Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji. | Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.  Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.  W tym czasie przedstawiciel Wykonawcy:   * zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. * dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:  1. zastosowanej technologii serwerów 2. zastosowanej technologii dyskowej 3. wirtualizacji 4. systemu backupu 5. zastosowanych rozwiązań aplikacyjnych   Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania. |
|  | Opracowanie dokumentacji powykonawczej | Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.   1. Wszelkie zmiany w stosunku do Dokumentacji systemu 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. |
|  | Opieka serwisowa | Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych. |

## Diagnoza cyberbezpieczeństwa

|  |
| --- |
| Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowy Powiat", opisanymi na stronie <https://www.gov.pl/web/cppc/cyfrowy-powiat>  Wykonawca musi wykonać usługę zgodnie zakresem oraz z aktualną wersją formularza stanowiącym załącznik do dokumentacji konkursowej. załączniku nr  Załącznik\_nr\_8\_-\_Formularz\_informacji\_związanych\_z\_przeprowadzeniem\_diagnozy\_cyberbezpieczeństwa  Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. |